FUJITSU

FUJITSU Integrated System HA Database Ready

利用ガイド

J2UL-1784-02Z0(00)
2014年5月

適用モデル：SX2

まえがき

本書の目的

本書は、FUJITSU Integrated System HA Database Ready(以降、HA Database Readyと略します)の概要と、セットアップおよび運用方法の概要について説明しています。

本製品の購入を検討されている方、または本製品を初めて使用される方は本書をご一読ください。

本書の適用モデル

本書が適用されるモデルは、SX2です。

本書の読者

本書は、以下の読者を対象としています。

- HA Database Readyの概要を知りたい方
- HA Database Readyのセットアップを担当する方
- HA Database Readyの運用管理を担当する方

本書の構成

本書は以下の構成になっています。

第1章 HA Database Readyの概要

HA Database Readyの特長と機能の概要について説明しています。

第2章 セットアップ

HA Database Readyのセットアップについて説明しています。

第3章 運用

運用操作を行うためのGUIツールである、Appliance Managerを使用したHA Database Readyの運用について説明しています。

付録A メッセージ一覧

HA Database Ready運用中に出力されるメッセージの一覧を示しています。

付録B 端末の条件

HA Database Readyのセットアップまたは運用に使用する端末の条件と、Webブラウザの設定を説明しています。

付録C 使用可能な文字コード一覧

使用可能な文字コードの一覧を掲載しています。

付録D 運用の詳細設定

HA Database Readyのセットアップ完了後に設定内容を確認する方法や、運用環境を変更する方法を説明しています。

付録E 運用管理サーバとの連携

運用管理サーバと連携する場合の設定方法を説明しています。

付録F Systemwalker Centric Managerの設定と運用

Systemwalker Centric ManagerからHA Database Readyの運用を管理する場合の基本的な設定と運用方法を説明しています。

付録G サーバへのログイン方法

サーバにログインする方法を説明しています。

付録H 購入時の状態

HA Database Readyを構成する機器の購入時の状態を説明しています。

付録I デザインシート

HA Database Readyの設定に使う値の一覧です。

付録J トラブルシューティング

製品名の表記

本書では、以下の製品名称を略称で表記しています。

略称	正式名称
HA Database Ready	FUJITSU Integrated System HA Database Ready

略語の表記

本書では、以下の略語を使用しています。

略称	製品名称
Windows Server 2008	Microsoft(R) Windows Server(R) 2008 Standard、 Microsoft(R) Windows Server(R) 2008 Enterprise、 Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V、 Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V、 Microsoft(R) Windows Server(R) 2008 R2, Standard、 Microsoft(R) Windows Server(R) 2008 R2, Enterpriseおよび Microsoft(R) Windows(R) Small Business Server 2011 Essentials
Windows Server 2012	Microsoft(R) Windows Server(R) 2012 Datacenter、 Microsoft(R) Windows Server(R) 2012 Standard、 Microsoft(R) Windows Server(R) 2012 Essentialsおよび Microsoft(R) Windows Server(R) 2012 Foundation
Windows	Windows Vista(R) Ultimate、 Windows Vista(R) Enterprise、 Windows(R) 7 Ultimate、 Windows(R) 7 Enterprise、 Windows(R) 7 Professional、 Windows(R) 8 Pro、 Windows(R) 8 Enterprise、 Windows(R) 8.1 Proおよび Windows(R) 8.1 Enterprise
	Windows Server 2008
	Windows Server 2012
Internet Explorer	Windows(R) Internet Explorer(R)
Internet Explorer 9.0	Windows(R) Internet Explorer(R) 9

マニュアルの留意事項

本マニュアルに記載している画面の例の一部は、読者にイメージをつかんでいただくためのものであり、完全な図ではありません。

商標

- Linuxは、Linus Torvalds氏の米国およびその他の国における登録商標あるいは商標です。
- Microsoft、Windows、Windows Serverまたはその他のマイクロソフト製品の名称および製品名は、米国Microsoft Corporationの米国およびその他の国における登録商標あるいは商標です。
- Red Hat、RPMおよびRed Hatをベースとしたすべての商標とロゴは、Red Hat, Inc.の米国およびその他の国における登録商標あるいは商標です。
- OracleとJavaは、Oracle Corporation およびその子会社、関連会社の米国およびその他の国における登録商標です。
- Interstage、ServerView、Symfoware、およびSystemwalkerは、富士通株式会社の登録商標です。

そのほか、文中の社名、商品名等は各社の商標または登録商標である場合があります。

輸出管理規制

本ドキュメントを輸出または提供する場合は、外国為替および外国貿易法および米国輸出管理関連法規等の規制をご確認の上、必要な手続きをおとりください。

出版年月および版数

2014年5月 第2版
2014年2月 初版

著作権表示

Copyright 2014 FUJITSU LIMITED

目　次

第1章 HA Database Readyの概要 1
1.1 HA Database Readyとは 1
1.1.1 ハードウェア構成 1
1.1.2 システム構成 3
1.1.3 基本スペック 6
1.2 HA Database Readyの特長 7
1.2.1 オープン性 7
1.2.2 高性能 7
1.2.3 簡単導入 7
1.2.4 簡単運用 8
1.3 HA Database Readyの運用 10

第2章 セットアップ 12
2.1 セットアップの準備 12
2.1.1 IPアドレスの準備 12
2.1.2 機器の準備 12
2.1.3 電源の投入 13
2.1.4 サーバのパスワード設定 15
2.1.5 故障監視のための設定 15
2.2 セットアップ 16
2.2.1 Appliance Managerへのログイン(セットアップ) 17
2.2.2 管理用のユーザーIDの設定 18
2.2.3 業務ネットワーク、内部ネットワーク設定 18
2.2.4 管理ネットワーク設定 20
2.2.5 データベースインターフェース設定 20
2.2.6 設定内容の確認 21
2.2.7 セットアップの完了 22
2.3 外部ネットワークとの接続 22

第3章 運用 24
3.1 管理端末の設定 24
3.2 Appliance Managerへのログイン 25
3.3 運用監視 26
3.4 警告・異常時の対処とリカバリー 30
3.5 運用変更 35
3.5.1 管理用のユーザーIDのパスワード変更 35
3.5.2 バックアップ 35
3.6 保守 36
3.6.1 修正適用 37
3.6.2 修正削除 39
3.6.3 調査資料の採取 41
3.6.4 ハードウェア部品交換 42
3.6.5 容量の追加 46
3.6.6 BIOS/ファームウェアの更新 48
3.6.7 保守ランプについて 49
3.7 データベースシステムの起動と停止 50
3.7.1 電源の投入 50
3.7.2 シャットダウン 50

付録A メッセージ一覧 52
A.1 FIS-HADBR_AMGRDBで始まるメッセージ 52
A.2 FIS-HADBR_AMGRCMEで始まるメッセージ 58

付録B 端末の条件 60
B.1 端末の条件 60
B.2 Webブラウザの設定 61

付録C 使用可能な文字コード一覧 63

付録D 運用の詳細設定 64
D.1 データベースインターフェースとIPアドレスの確認 64
D.2 データベースインターフェースの初期化 65
D.3 ネットワークの変更 66
D.4 管理ネットワークの経路設定 69
D.5 メッセージの消去 70
D.6 外部バックアップ 71
D.6.1 外部バックアップの事前準備 72
D.6.2 外部バックアップを用いたリカバリー 77
D.7 ホスト名の変更 80
D.8 格納データの暗号化 81
D.8.1 暗号化の事前準備 82
D.8.2 暗号化の設定 82
D.8.3 バックアップ 83
D.8.4 リカバリー 85
D.8.5 マスタ暗号化キーの変更 86
D.8.6 キーストアのパスフレーズの変更 87

付録E 運用管理サーバとの連携 88
E.1 運用監視 88
E.2 時刻補正 89
E.3 メール通知 90
E.3.1 メールの設定 90
E.3.2 通知されるメールの内容 92
E.4 文字管理 93
E.5 電源制御 94
E.5.1 電源の投入 95
E.5.2 電源状態の確認 96

付録F Systemwalker Centric Managerの設定と運用 98
F.1 運用準備 98
F.2 運用開始 102
F.3 運用時の注意 104
F.3.1 Systemwalkerコンソールでの表示名について 104
F.3.2 HA Database Ready内のCentric Manager(業務サーバ)の正常起動確認について 105
F.4 使用制約 105

付録G サーバへのログイン方法 109

付録H 購入時の状態 110
H.1 IPアドレス 110
H.2 ホスト名 110
H.3 時刻設定 111

付録I デザインシート 112

付録J トラブルシューティング 114
J.1 セットアップ中にトラブルが発生した場合の対処方法 114
J.1.1 STEP2 セットアップ 114
J.1.2 STEP3 動作確認 119

J.2 問合せ時に必要な情報 120
J.3 使用上の留意事項 120
J.3.1 サーバユニットの留意事項 120
J.3.2 外部接続スイッチの留意事項 120

索引 122

第1章 HA Database Readyの概要

本章では、HA Database Readyの特長と構成について説明します。

1.1 HA Database Readyとは

HA Database Readyは、最新のハードウェア(サーバ、ストレージ、ネットワーク)とデータベースソフトウェア(Symfoware Server)を一体化したデータベースサーバです。
HA Database Readyでは、高性能なオンライントランザクション処理に対応するため、最適な環境にチューニングされています。また、サーバ、ネットワーク、データベースを二重化することで高い信頼性を実現しています。

図1.1 HA Database Readyの外観

1.1.1 ハードウェア構成

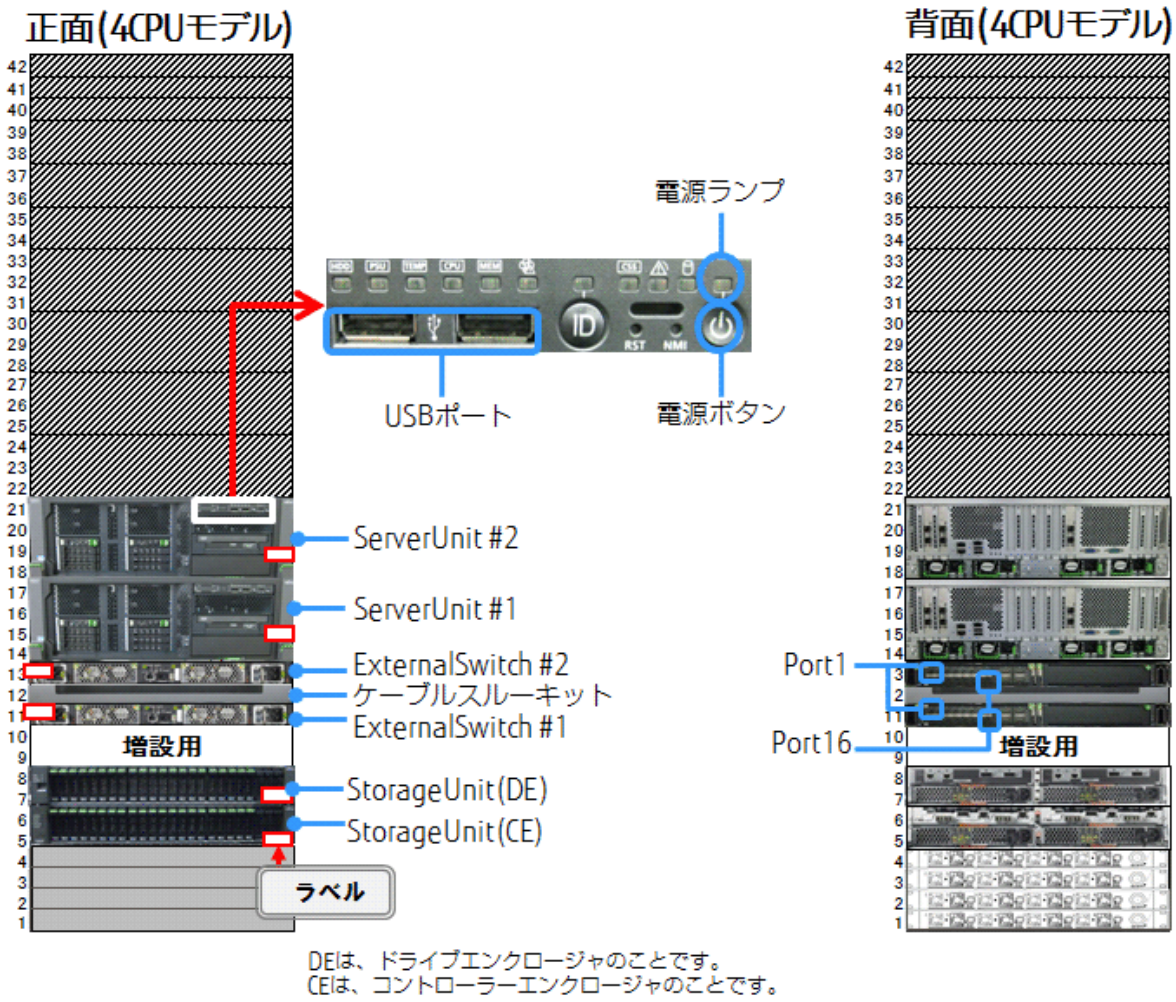
HA Database Readyを構成するスイッチ、サーバ、およびストレージは結線された状態で専用のラックに搭載されています。各装置の装置名は以下のとおりです。装置名を記載したラベルが各装置に貼付されておりますので、操作時に確認してください。

表1.1 装置名

装置	装置名
スイッチ	ExternalSwitch#1、ExternalSwitch#2
サーバ	ServerUnit#1、ServerUnit#2
ストレージ	StorageUnit

装置名、正面のイメージ、および背面のイメージを以下に示します。電源の投入は、ServerUnit#1の電源ボタンを利用します。ネットワークの接続はExternalSwitch#1とExternalSwitch#2のPort1およびPort16を使用します。

図1.2 正面と背面のイメージ



注意

本書では4CPUモデルで説明

HA Database Readyには、2CPUモデルと4CPUモデルがありますが、本書では4CPUモデルを例に説明します。
各モデルの構成要素の詳細と2CPUモデルの搭載例は“設置ガイド”を参照してください。

付属のDVD

HA Database Readyには、以下のDVDが付属されています。以下の用途で使用します。

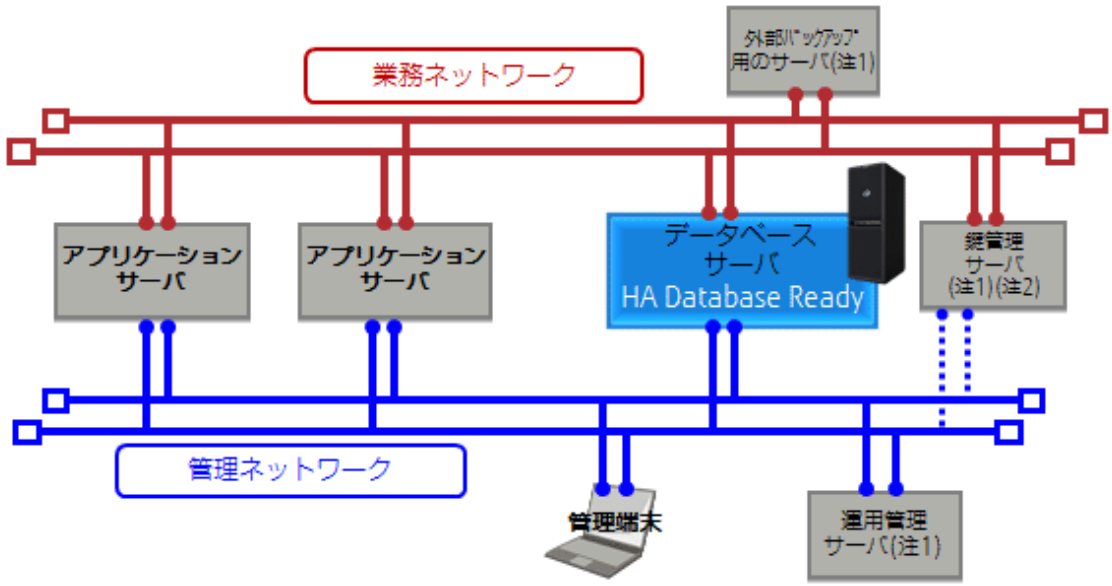
メディア名	用途
FUJITSU Integrated System HA Database Ready SX2 リカバリーメディア	故障時などに初期状態への復元を行う場合に使用します。
FUJITSU Integrated System HA Database Ready クライアントメディア for Open SQL V1.1.0	HA Database Readyのクライアント機能をインストールする場合に使用します。
FUJITSU Integrated System HA Database Ready クライアントメディア for Native SQL V1.1.0	

メディア名	用途
FUJITSU Integrated System HA Database Ready オンラインドキュメント V1.1.0	HA Database Readyのマニュアルを参照する場合に使用します。
UpdateAdvisor(ミドルウェア)	HA Database Readyのクライアント機能に対し、修正を適用する場合に使用します。

1.1.2 システム構成

HA Database Readyのシステム構成例を説明します。

図1.3 HA Database Readyのシステム構成例



注1) 必須のサーバではありません。必要に応じてご用意ください。
注2) 鍵管理サーバは、業務ネットワークまたは管理ネットワークのどちらに配置しても構いません。

管理端末

HA Database Readyの運用管理や修正適用のための端末です。

管理ネットワーク

HA Database Readyと、管理端末や運用管理サーバとを接続するネットワークです。HA Database Readyの運用監視で使用します。
1GbEで、Active-Standby方式の経路二重化に対応しています。

業務ネットワーク

HA Database Readyとアプリケーションサーバとを接続するネットワークです。業務で使用します。
1GbEまたは10GbEで、Active-Standby方式の経路二重化に対応しています。

上記の構成でHA Database Readyをデータベースシステムとして運用できますが、以下のように、お客様の運用環境と連携が可能です。

運用管理サーバ

HA Database Readyやアプリケーションサーバの運用管理を行うためのサーバです。以下の機能を持つサーバと連携できます。

・ 運用監視
HA Database Readyの運用を監視します。以下のソフトウェアのいずれかが必要です。

ー Systemwalker Centric Manager Enterprise Edition V13.6(マネージャー)

ー Systemwalker Centric Manager Standard Edition V13.6(マネージャー)

・ 時刻補正
NTP(Network Time Protocolの略です)で時刻を同期します。

・ メール通知
SMTP(Simple Mail Transfer Protocolの略です)で状態をメールで通知します。

・ 文字管理
外字を一元管理します。文字管理ソフトウェアとして、以下のソフトウェアが必要です。

ー Interstage Charset Manager Standard Edition V9(9.3)以降

・ 電源制御
iRMCで電源を制御します。

外部バックアップ用のサーバ

災害発生時に備えて、データベース資源をバックアップするためのサーバです。

鍵管理サーバ

データ暗号化を行う場合に、キーストアをバックアップするためのサーバです。
鍵管理サーバはデータベース資源ですので、業務ネットワークに配置します。ただし、業務への影響を避ける場合は、管理ネットワークに配置してください。

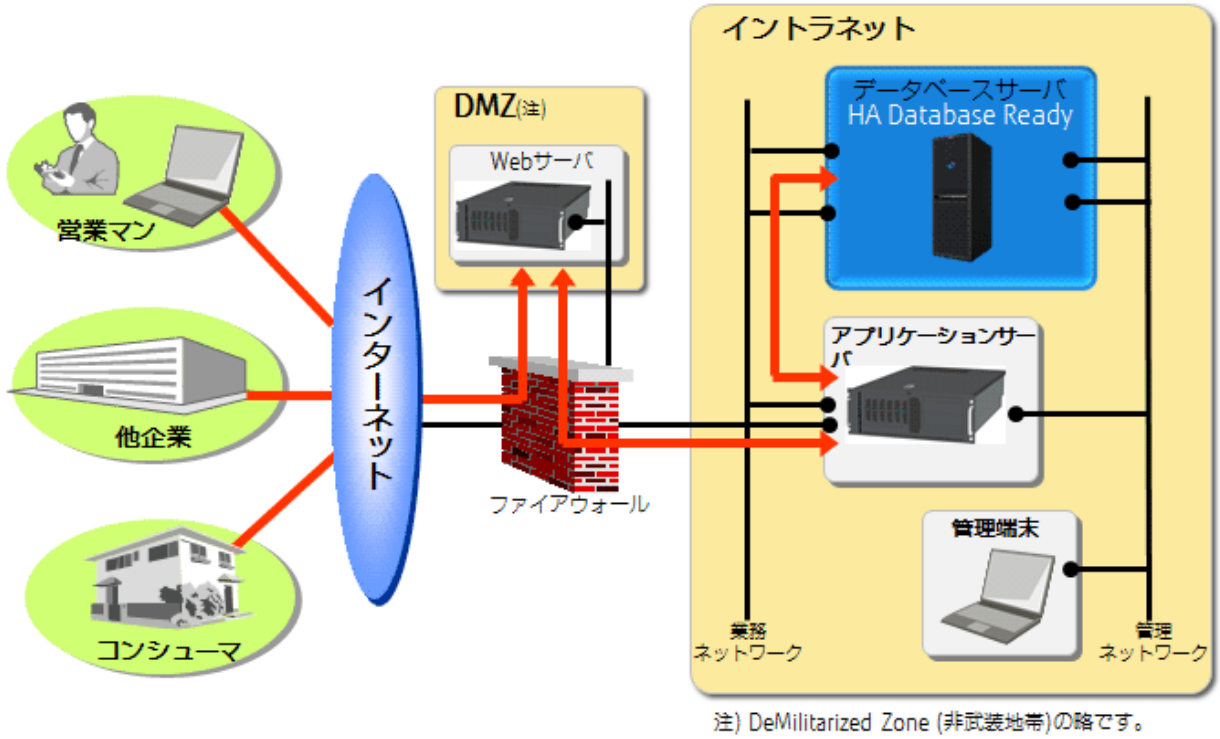
参照

HA Database Readyの内部のネットワーク構成については、“設置ガイド”の“ネットワーク接続構成”を参照してください。

インターネットを利用した接続形態

HA Database Readyのシステム構成を設計する場合、以下の点に注意してください。

図1.4 インターネットを利用した接続形態のシステム構成例



インターネットを利用した接続形態では、外部の不正アクセスからデータを守るために、HA Database Readyおよびアプリケーションサーバはイントラネット内に配置してください。

さらに、ファイアウォールにDMZという第3のネットワークを追加して、そのネットワークに社外公開用のWebサーバを設置することにより、Webサーバをファイアウォールの管理下に置き、不正アクセスを防止します。

ファイアウォールを超えるアクセスは、アプリケーションサーバを経由した通信方法を採用します。

また、ネットワーク上のデータ漏洩や改ざんからデータを守るために、アプリケーションサーバより外部ではSSLなどの暗号化通信を使用してください。

参考

HA Database Readyでは、Linuxのパケットフィルタリング機能であるiptablesおよびip6tablesを用いることができます。

初期設定ではHA Database Readyがイントラネット内に配置されることを想定しているため、すべてのアクセスを許可する設定になっています。

HA Database Ready上のiptablesおよびip6tablesを変更する場合、各サーバユニットにログインし、変更作業を行なってください。

注意

- HA Database Ready上のiptablesを変更する場合は、事前に十分な検証を行なってください。
- HA Database Ready上のiptablesは、HA Database Readyを構成する機器からの通信が正常に行えるように設定する必要があります。各機器のIPアドレスからのアクセスを許可するルールを適切に設定するようにしてください。HA Database Readyを構成する機器間の通信が正常に行えない場合、HA Database Readyは動作しません。

参照

- サーバユニットへのログイン方法については、“付録G サーバへのログイン方法”を参照してください。
- HA Database Readyを構成する機器のIPアドレスについては、“D.1 データベースインターフェースとIPアドレスの確認”を参照してください。

1.1.3 基本スペック

HA Database Readyの基本スペックを説明します。

項目			仕様							
			2CPUモデル		2CPUモデル+容量増設オプション(注1)		4CPUモデル		4CPUモデル+容量増設オプション(注1)	
データベースインターフェースの種別(注2)			Open SQL	Native SQL	Open SQL	Native SQL	Open SQL	Native SQL	Open SQL	Native SQL
データベース規模	最大ユーザーデータ量(テラバイト)		1.8	1.6	3.9	3.6	3.9	3.4	5.9	5.5
	DBバッファ割当て量(ギガバイト)		48	30	48	30	48	30	48	30
	最大接続数		4,000							
ハードウェア	Server Unit (1台当たり)	CPU種類 (クロック/コア数/キャッシュサイズ)	インテル® Xeon® プロセッサE5-4650 (2.70GHz,8コア,20メガバイト)							
		CPU数(総コア数)	2(16コア)				4(32コア)			
	Server Unit搭載のPCIe SSD性能	読取り帯域幅	3.0ギガバイト/秒							
		書込み帯域幅	2.5ギガバイト/秒							
		シーケンシャル読取りIOPS(8KB) (注3)	35,000							
		シーケンシャル書込みIOPS(8KB) (注3)	87,000							
		ランダム読取りIOPS(8KB) (注3)	35,000							
		ランダム書込みIOPS(8KB) (注3)	76,000							
		ランダム読み書き混在のIOPS(8KB) (注3)	75,000							
ソフトウェア	基本ソフトウェア		Red Hat Enterprise Linux 6.4(for Intel64)							
	データベースソフトウェア		Open SQLの場合:Symfoware Server Standard Edition V12 Native SQLの場合:Symfoware Server Enterprise Edition V11							
	文字管理ソフトウェア		Interstage Charset Manager Standard Edition Agent V9.3 (64bit版)							
	サーバ監視ソフトウェア		ServerView Operations Manager for Linux V6.21							
	運用監視ソフトウェア(業務サーバ)		Systemwalker Centric Manager Standard Edition V13.6 (業務サーバ用)							

注1) 容量増設オプションを追加した場合です。
注2) データベースインターフェースによって、値が異なります。Open SQLとNative SQLについては“1.2.1 オープン性”を参照してください。
注3) “IOPS（8KB)”は、8KBのデータを1秒間に読込み・書込みできる回数のことです。

1.2 HA Database Readyの特長

HA Database Readyの特長を説明します。

1.2.1 オープン性

オープンスタンダードなインターフェースを採用しており、さまざまな開発環境を活用してアプリケーションの生産性や移行性が向上します。

データベースインターフェース

HA Database Readyは以下の2つのインターフェースをサポートしています。

- Open SQL
  PostgreSQL 9.2互換のインターフェースです。詳細については、“業務開発ガイド(Open SQL編)”を参照してください。
- Native SQL
  Symfoware Serverのインターフェースです。詳細については、“業務開発ガイド(Native SQL編) ”を参照してください。

1.2.2 高性能

HA Database Readyは、最新のハード技術を活用し、性能を向上するために最適な資源配置をしています。

PCIe SSDを活かした高性能

富士通の高性能PRIMERGYサーバに、高速なI/Oを実現するPCIe SSDを搭載しています。データベースシステム全体をPCIe SSD上に配置することで、大量のトランザクションやバッチの高速処理を実現しています。

1.2.3 簡単導入

HA Database Readyでは、ハードウェアとソフトウェアが一体化されている製品のため、製品導入時の設定作業が簡素化されています。

セットアップ

OSおよびソフトウェアがインストール済みの状態で提供されるため、環境設定は、GUI(Appliance Manager)のウィザードにより、簡単な操作でのセットアップ作業が可能です。

図1.5 Appliance Managerのネットワーク環境の設定画面

セットアップについては、“第2章 セットアップ”を参照してください。

高可用システム

HA Database Ready導入時に、高可用システムに必要なバックアップ機能や冗長化のセットアップを意識する必要がありません。また、HA Database Readyが自動的にバックアップを取得するため、バックアップ運用に必要とされる、運用設計が不要です。

1.2.4 簡単運用

運用の自動化により、SEを前提としない、データベースシステムの運用が可能です。

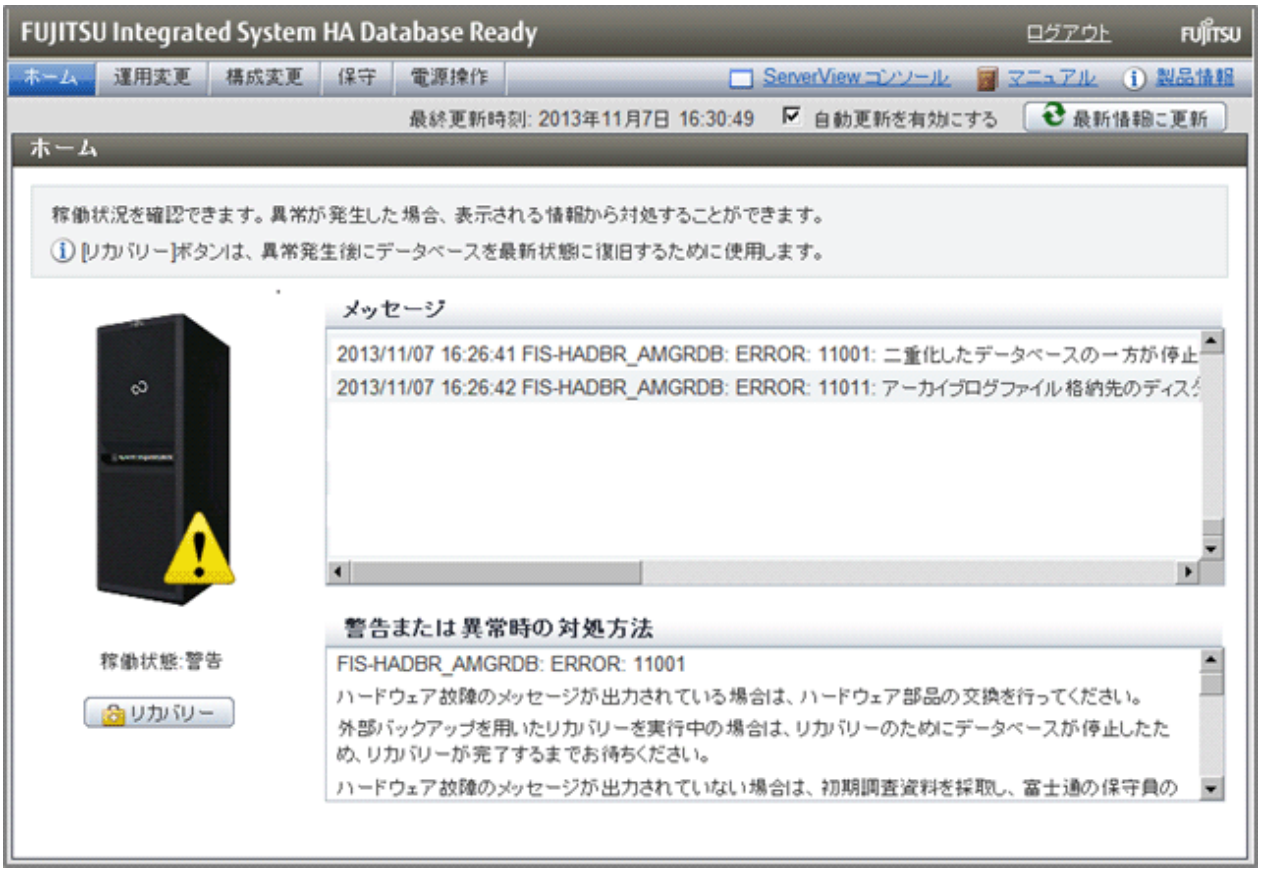
自動的な業務継続

データベースのバックアップ機能やシステム(サーバ、ネットワーク、データベース)の冗長化構成が標準搭載されています。ハードウェア故障などの異常が発生した場合、自動で運用対象とするサーバが切り替わります。

ワンクリックリカバリー

ハードウェア部品故障などの異常が発生した場合、ハードウェア部品の交換後、Appliance Managerでのワンクリック操作でリカバリーが可能です。データベースの専門的な知識がなくても、リカバリー操作を行うことができます。

図1.6 Appliance Managerのリカバリー操作画面



運用中の容量追加

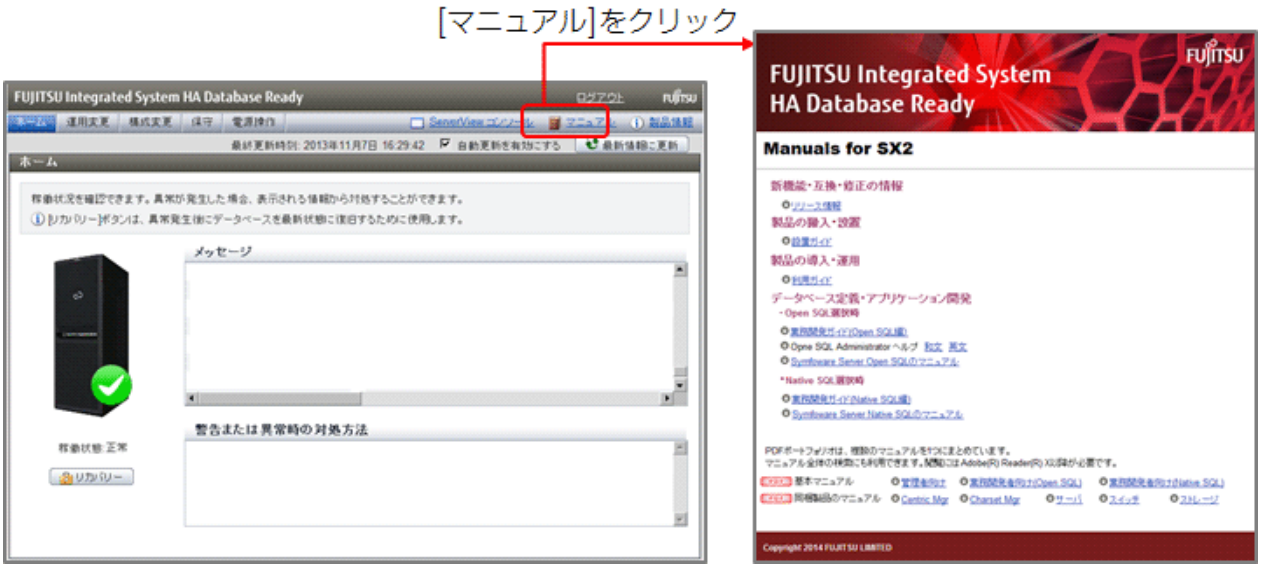
運用中にデータベースの容量が不足した場合、容量増設オプションを購入することでデータベースの容量を拡張することができます。

運用中の容量追加の手順については、“3.6.5 容量の追加”を参照してください。

マニュアルの参照

HA Database Readyのオンラインマニュアルは、Appliance Managerから参照できます。

図1.7 Appliance Managerからのマニュアルへのリンク



1.3 HA Database Readyの運用

HA Database Readyの運用を説明します。

データベースシステムでは、何らかのトラブルが発生した場合に、データの損失を最小限に防ぎ、迅速に業務を再開させることが重要です。HA Database Readyでは、不測の事態に備え、バックアップや稼働状態の監視を自動的に行っています。
異常が発生した場合は、データベースを正常な状態に戻すための対処をAppliance Managerで行うことができます。
また、運用環境の変更に対応するため、運用開始後の環境変更も柔軟に行えます。
さらに、HA Database Readyでは、ローリングアップデートによるソフトウェアの修正適用が可能です。

データベースシステムの起動/停止

設置場所の停電、ネットワーク環境の変更など、HA Database Readyのシャットダウンや電源の投入が必要となる場合があります。HA Database Readyでは、HA Database Readyの電源操作とデータベースシステムの起動/停止が連動しているため、データベースシステムの起動/停止の操作が不要です。データベースシステムの起動は、ServerUnit#1の電源ボタンを押して行います。
また、iRMCの電源制御機能を使ってリモートから電源を投入できます。“E.5.1 電源の投入”を参照してください。

運用監視

HA Database Readyでは、以下をチェックすることで、HA Database Ready の運用状態を監視しています。
・データベースの稼働状況
・バックアップの稼働状況
・ハードウェアの状態異常
運用監視の手順については、“3.3 運用監視”を参照してください。

また、以下の監視方法に対応しています。

- Systemwalker Centric Managerと連携した監視
  Systemwalker Centric Managerの運用管理サーバ、または運用管理サーバ経由で他社の運用管理製品から、HA Database Readyの稼働状態を管理できます。運用管理サーバの詳細については、“E.1 運用監視”を参照してください。

- 稼働状態をメールで自動送信
  お客様のSMTPサーバと連携して、システムの稼働状態を通知するメールを自動送信できます。設定方法については、“E.3 メール通知”を参照してください。

バックアップ

HA Database Readyでは、データベース資源をストレージに自動で退避します。購入時の状態では、毎日午前1時に、自動的にバックアップが開始するように設定されていますが、運用に応じて、バックアップ時刻の変更や手動バックアップが可能です。
バックアップ時刻の変更や手動バックアップの手順については、“3.5.2 バックアップ”を参照してください。
また、災害発生時に備えて、ストレージに自動退避しているデータベース資源を、外部のバックアップ環境に退避することもできます。外部バックアップの詳細については、“D.6 外部バックアップ”を参照してください。

モニタリング

データベースの容量監視や、性能情報のモニタリング、データベースのチューニングを行います。使用するデータベースインターフェースに合わせて、“業務開発ガイド(Open SQL編)”または、“業務開発ガイド(Native SQL編)”を参照してください。

異常時の対処

ハードウェア故障やシステムダウンなど、HA Database Readyに異常が発生した場合、データベースを正常な状態に復旧させる必要があります。バックアップとアーカイブログを利用することで、データベースを最新の状態まで復元できます。
アーカイブログは、HA Database Readyにより、ストレージ上に蓄積されるデータベースのトランザクションの更新履歴です。
異常発生時の対処については、“3.4 警告・異常時の対処とリカバリー”を参照してください。

また、弊社保守員による対処が必要なトラブルが発生した場合に、発生箇所の特定に必要な資料を採取できます。その方法については、“3.6.3 調査資料の採取”を参照してください。

ハードウェア部品交換

ハードウェア部品が故障した場合など、ハードウェアの部品を交換します。弊社保守員がハードウェアの部品を交換した後、Appliance Managerでリカバリー操作を行います。“3.6.4 ハードウェア部品交換”を参照してください。

運用環境の変更

運用開始後に、以下の運用環境を変更できます。

- パスワード
  セキュリティ確保のためにパスワードを変更する場合は、“3.5.1 管理用のユーザーIDのパスワード変更"を参照してください。
- データベースインターフェース
  データベース設計変更やセットアップ手順の誤りのためデータベースインターフェースを変更する場合は、“D.2 データベースインターフェースの初期化”を参照してください。
- HA Database Readyのネットワーク環境
  HA Database Readyの設置場所を移動するため、ネットワーク環境を変更する場合は、“D.3 ネットワークの変更”を参照してください。
- HA Database Readyの時刻設定
  HA Database Readyのすべての機器は、ServerUnit#1と同期するようにあらかじめ設定されています。お客様のNTPサーバとHA Database Readyの時刻を同期することも可能です。“E.2 時刻補正”を参照してください。
- 外字管理
  データベースで外字を扱う場合は、Interstage Charset Managerを使用します。“E.4 文字管理”を参照してください。
- サーバのホスト名の変更
  同一のシステム内で複数のHA Database Readyを運用したい場合や、独自の命名規約に沿ったホスト名でHA Database Readyを運用したい場合は、サーバのホスト名を変更できます。ServerUnit#1、ServerUnit#2のホスト名を変更する場合は、“D.7 ホスト名の変更”を参照してください。

ソフトウェアの修正適用

HA Database Readyに組み込まれたソフトウェアに対する障害を修正します。
修正は、SupportDesk契約時に弊社から通知されたサイトで公開されます。基本ソフトウェアの修正は、弊社が提供する修正情報で指定する修正だけ適用できます。
修正適用は、Appliance Managerで実施します。“3.6.1 修正適用”を参照してください。

BIOS/ファームウェアの更新

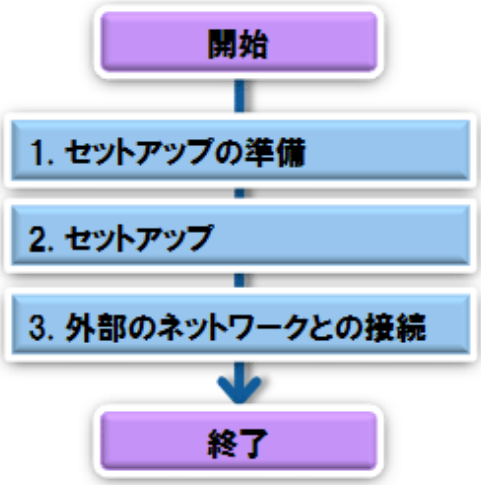
BIOS/ファームウェアの更新では、データベースの運用を停止して行うため、業務の影響を考慮して、作業計画を立てます。
システム安定稼働のため、常に最新BIOS/ファームウェアの適用をお願いします。
なお、サーバユニットおよび外部接続スイッチの最新モジュールのダウンロード、および適用作業につきましては、お客様自身で実施してください。ストレージユニットのファームウェアの更新は、弊社保守員が実施します。
作業の詳細については、“3.6.6 BIOS/ファームウェアの更新”を参照してください。

格納データの暗号化

HA Database Readyでは、透過的データ暗号化による格納データの保護(以降、格納データの暗号化と呼びます)を提供します。格納データを暗号化することで、盗難による情報漏洩を防ぎます。データベースインターフェースとしてOpen SQLインターフェースを選択した場合だけ利用できます。“D.8 格納データの暗号化”を参照してください。

第2章 セットアップ

本章では、HA Database Readyのセットアップについて説明します。
セットアップは、機器の設置後に行います。セットアップ作業の流れは以下のとおりです。



注意

セットアップ中にトラブルが発生した場合の対処方法については“付録I トラブルシューティング”を参照してください。

2.1 セットアップの準備

HA Database Readyのセットアップを開始する前に必要な準備作業を以下に示します。

2.1.1 IPアドレスの準備

“設置ガイド”の“外部ネットワーク接続”を参照し、HA Database Readyと外部ネットワークの接続構成を決めてください。

セットアップには、デザインシートを利用すると便利です。デザインシートは“付録I デザインシート”にありますので、印刷してご利用ください。デザインシートを参照して、IPアドレスを準備し、データベースとユーザーIDを決めてください。

ポイント

本マニュアルでは、*斜体*は、お客様の環境に合わせて変更する値を示しています。

2.1.2 機器の準備

準備する機器

HA Database Readyのセットアップのために、以下の2点を用意してください。

- セットアップ用PC
  HA Database Readyのセットアップ時だけ使用します。用意する端末の条件について“B.1 端末の条件”を参照してください。

・ LANケーブル
セットアップ用PCをHA Database Readyに接続するために使用します。ツイストペアケーブル(カテゴリー5e以上)が必要です。

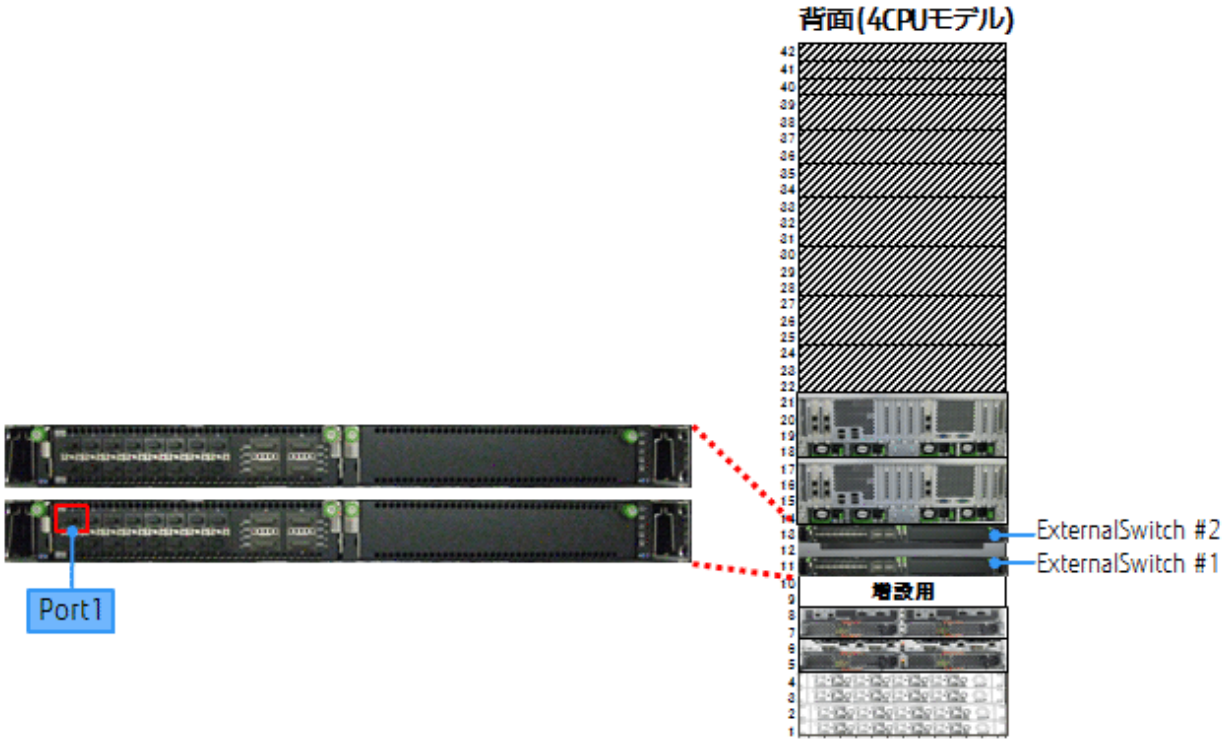
結線状態の確認

装置間を接続するネットワークケーブルが抜けていないか、または緩んでいないか確認してください。
結線状態に不具合がある場合は、弊社保守員までご連絡ください。

セットアップ用PCの接続

以下の手順で、セットアップ用PCをHA Database Readyに接続します。

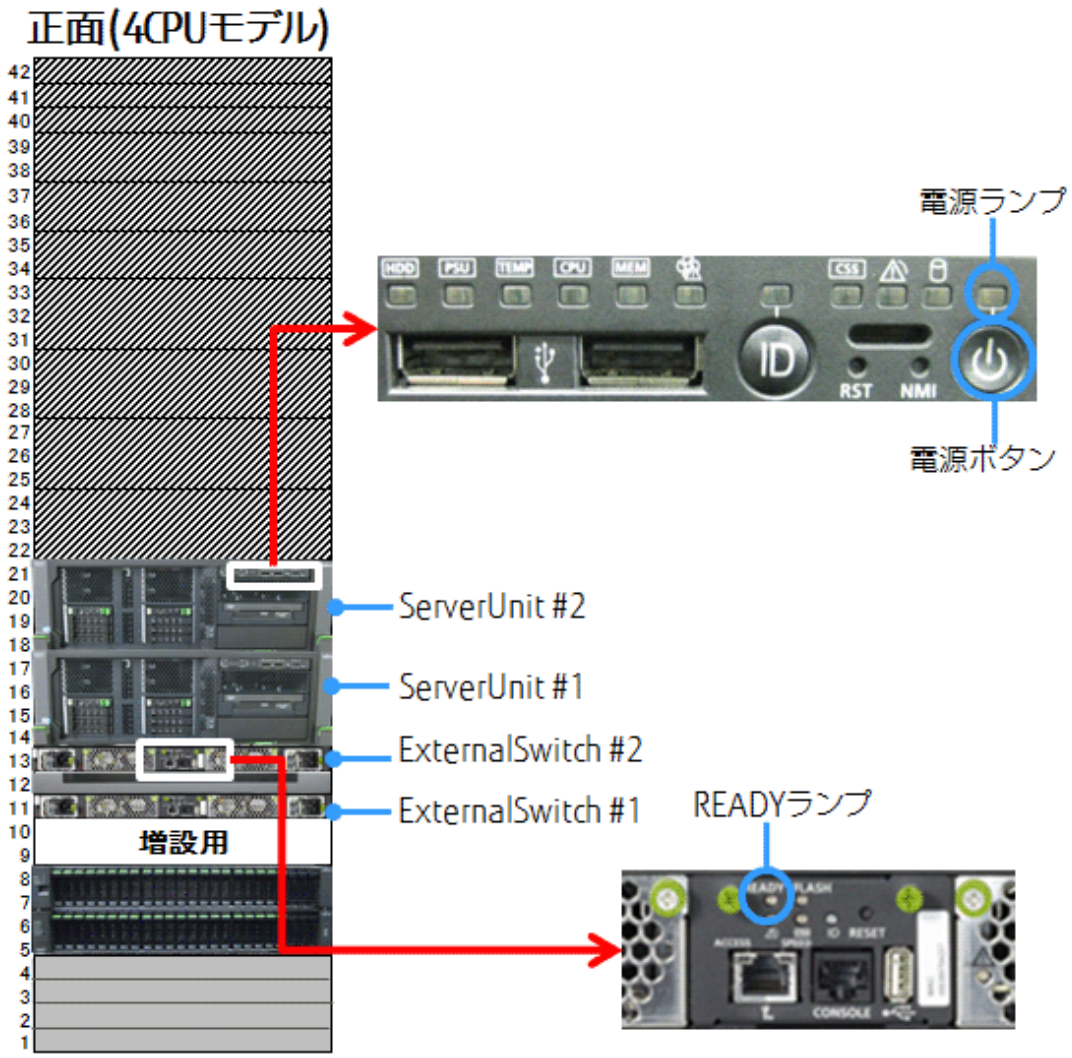
1. セットアップ用PCのIPアドレスを“192.168.1.30”、サブネットマスクは“255.255.255.0”に設定してください。
2. LANケーブルを使って、セットアップ用PCをExternalSwitch#1のPort1に接続します。



2.1.3 電源の投入

HA Database Readyの電源の投入方法を説明します。以下の手順で電源を投入してください。

図2.1 電源ボタンと電源ランプの位置



1. ラック前面の扉を開けて、ExternalSwitch#1とExternalSwitch#2のREADYランプが緑色に点灯していることを確認します。
2. ServerUnit#1とServerUnit#2の電源ランプを確認します。

   ー オレンジ色に点灯…電源が入っていません(スタンバイ)。

   ー 緑色に点灯…電源が入っています。
3. ServerUnit#1とServerUnit#2の電源ランプがオレンジ色に点灯している場合は、ServerUnit#1の電源ボタンを押してHA Database Readyを起動します。このボタンを押すだけで、ServerUnit#1、ServerUnit#2、およびStorageUnitの電源が入ります。

   参考

   ServerUnit#2の電源ボタンを押しても、ServerUnit#1、ServerUnit#2、およびStorageUnitの電源が入ります。
4. 以下を見て、各装置の起動状況を確認します。正常の場合、約10分以内に以下の状態になります。

   ー ServerUnit#1、ServerUnit#2およびStorageUnitの電源ランプが緑色に点灯

   電源ボタンを押してからシステムが起動するまで約15分かかります。15分は目安です。

2.1.4 サーバのパスワード設定

以下の手順で、サーバのスーパーユーザー(root)のパスワードを設定します。

1. セットアップ用PCから、端末エミュレータソフトウェアを使って、 ServerUnit#1にスーパーユーザー(root)でアクセスします。
   アクセス時のIPアドレスは、“192.168.1.10”です。購入時のスーパーユーザーのパスワードは、以下を参照してください。

項目	値
接続プロトコル	SSH2プロトコル
アクセス時のユーザーID	root
パスワード	rootroot
ログイン時のロケール	ja_JP.UTF-8

2. 以下のOSのpasswdコマンドを入力して、“付録I デザインシート”の“表I.3 ユーザーID”で決めたパスワードを設定します。パスワードは、6文字以上の長さが必要です。

```
# passwd
ユーザー root のパスワードを変更。
新しいパスワード:
新しいパスワードを再入力してください:
passwd: 全ての認証トークンが正しく更新できました。
```

3. logoutコマンドを入力して、ログアウトします。

```
# logout
```

4. ServerUnit#2にスーパーユーザー(root)でアクセスします。アクセス時のIPアドレスは、“192.168.1.11”です。
5. 手順2.～3.を繰り返します。ServerUnit#1で設定したパスワードと同じパスワードを指定してください。

2.1.5 故障監視のための設定

装置の故障監視のため、以下の手順で、サーバの設定を行います。

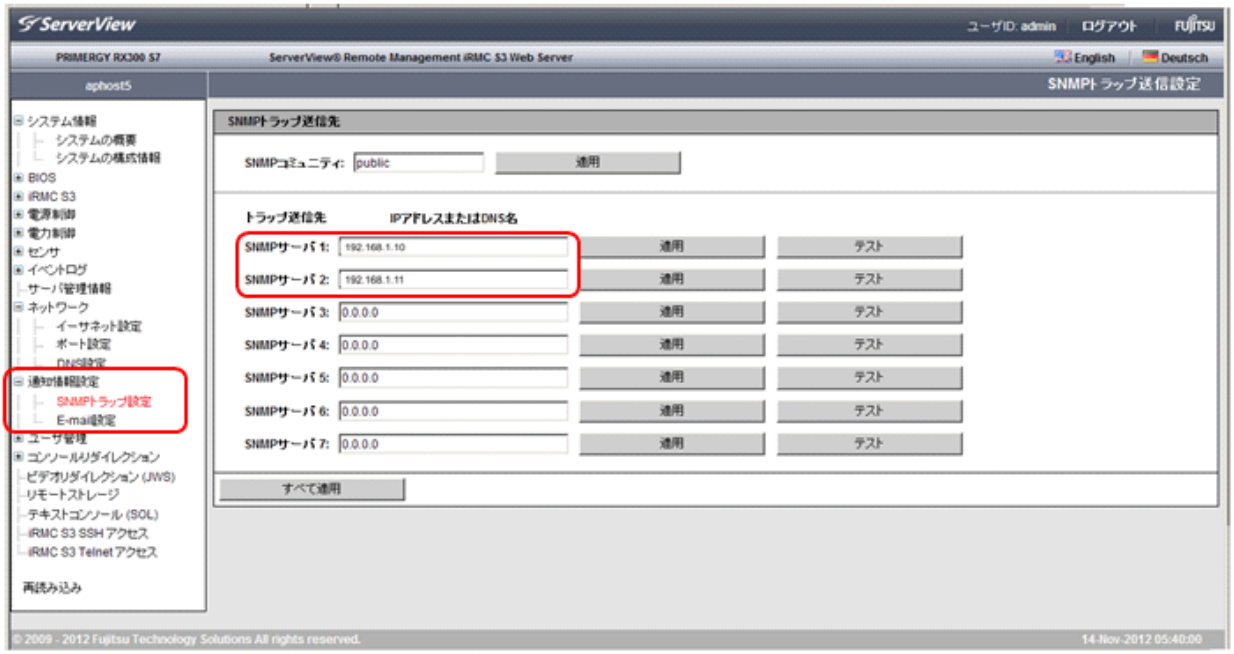
1. セットアップ用PCで、Webブラウザを起動します。
2. Webブラウザのアドレスバーに、以下のURLを入力します。

```
http://192.168.1.20/
```

   認証画面が表示されます。ユーザー名:「admin」、パスワード:「admin」でアクセスしてください。

3. 認証が完了するとServerViewの画面が表示されます。
   画面が英語で表示されている場合、画面右上の[日本語]リンクをクリックしてください。

4. 左画面のナビゲーションエリアのメニューで[通知情報設定]の[SNMPトラップ設定]を選択すると、以下の画面が表示されます。



5. 右画面の[SNMPトラップ送信先]の[IPアドレスまたはDNS名]欄に以下の値を指定し、[すべて適用]ボタンをクリックしてください。

   ー [SNMPサーバ1] : “付録I デザインシート”の“表I.1 IPアドレス”(10) (*192.168.1.10*)

   ー [SNMPサーバ2] : “付録I デザインシート”の“表I.1 IPアドレス”(11) (*192.168.1.11*)

6. ユーザー名:「admin」のパスワードを必ず変更してください。パスワードを変更するには、左画面のナビゲーションエリアのメニューで [ユーザ管理]を選択し、[iRMC S3ユーザ管理]をクリックします。次に、右画面の[名前]がadminのリンクをクリックして、パスワードを“付録I デザインシート”の“表I.3 ユーザーID”で決めた値に変更してください。

   パスワードを忘れると、本設定の変更ができなくなりますので、パスワードは忘れないようにしてください。

   注意

   ユーザー名:「admin」以外のユーザーの設定を変更しないでください。変更した場合、HA Database Readyは動作しません。

7. 画面右上の[ログアウト]リンクをクリックしたあと、[ログアウト]ボタンをクリックしてログアウトします。

8. セットアップ用PCのWebブラウザのアドレスバーに、以下のURLを入力します。

   ```
   http://192.168.1.21/
   ```

   認証画面が表示されますので、ユーザー名:「admin」、パスワード:「admin」でアクセスしてください。

9. 手順3.～7.を実行してください。

2.2 セットアップ

HA Database Readyのセットアップの手順を説明します。

2.2.1 Appliance Managerへのログイン(セットアップ)

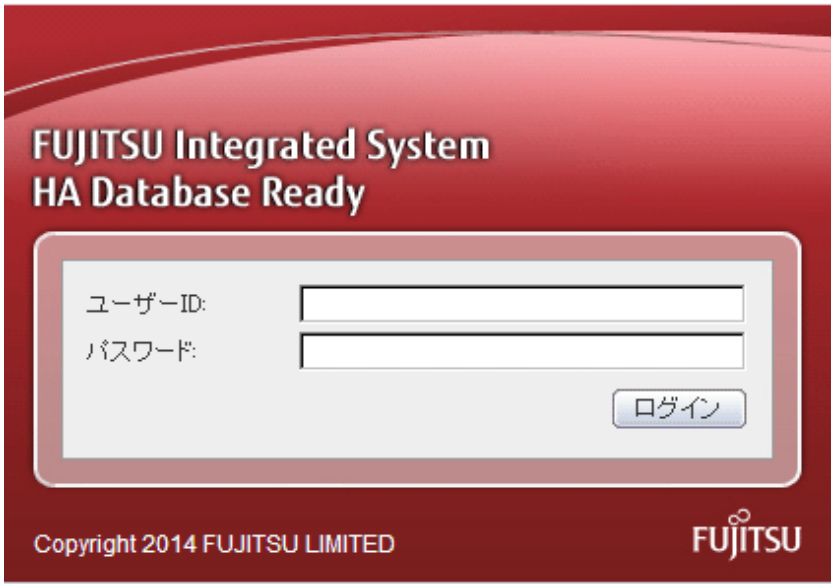
セットアップ用PCからAppliance Managerを起動して、セットアップを実施します。以下の手順で、Appliance Managerを起動してください。

1. セットアップ用PCで、Webブラウザを起動します。
2. Webブラウザのアドレスバーに、以下のURLを入力します。この値は、購入時の設定値に基づくURLです。

   ```
   https://192.168.1.10/appmgr/
   ```

   「このWebサイトのセキュリティ証明書には問題があります。」という警告が表示されますが、[このサイトの閲覧を続行する]リンクを選択し、ログインを続行してください。

   [ログイン]画面が表示されます。



3. ユーザーID「administrator」とパスワード「administrator」を入力し、[ログイン]ボタンをクリックします。

注意

- ログインするとWebブラウザのURLに“index.jsp”が付加されて“https://*管理用のIPアドレス*/appmgr/index.jsp”と表示されますが、ログインする時にはURLに“index.jsp”を指定しないでください。指定した場合、サーバの状態が誤って判断されて、機能制限された状態でログインする場合があります。
  URLに“index.jsp”を指定してログインした場合は、ログアウトし、“index.jsp”なしのURLで再度ログインしてください。
- Appliance Managerの操作中は、Webブラウザの機能で[前のページに移動する]および[現在のWebページを更新する]の操作は行わないでください。誤って操作した場合は、Webブラウザを終了し、再度、Appliance Managerへのログインから実施してください。
- Appliance Managerのセットアップの各画面では、[キャンセル]ボタンまたは[閉じる]ボタンをクリックすると、セットアップ処理が中止されます。キャンセルしてよいのかを確認するポップアップメッセージが表示されますので、[OK]ボタンをクリックするとWebブラウザが終了します。セットアップを中止した場合、中止時のセットアップの進行状況により、各画面で入力したデータが破棄される場合があります。破棄されたデータは再度入力しなおしてください。
- Appliance Managerのセットアップ中に、別のWebブラウザや別のウィンドウからAppliance Managerにログインしないでください。
- Appliance Managerのセットアップが完了する前に、Webブラウザを閉じる操作などで処理が中断した場合は、再度、Appliance Managerへのログイン以降の手順を実施して、セットアップしてください。

- “2.2.7 セットアップの完了”の[セットアップ状況]画面において、[管理用IDのユーザーIDの設定]が成功した後に画面を閉じた場合、セットアップが完了していなくても、再度ログインする際には新しく設定したユーザーIDとパスワードを使用してください。
- 一定時間(約30分)ブラウザを操作しなかった場合、タイムアウトとなり、次の操作でログイン画面に戻ります。

参照

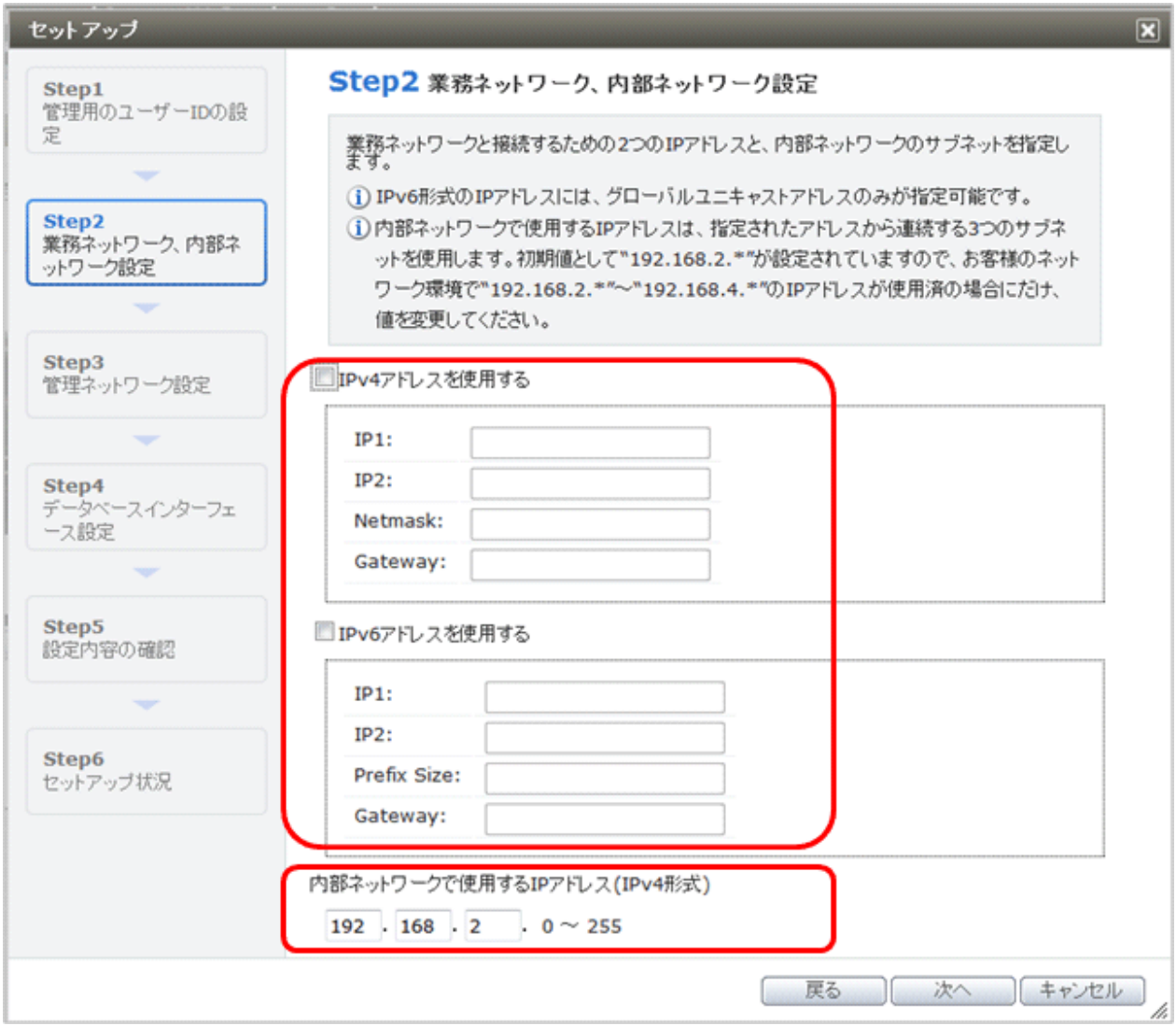
Webブラウザ上でAppliance Managerの表示が崩れる場合、またはセキュリティのエラーメッセージが表示される場合は、“B.2 Webブラウザの設定”を参照して、Webブラウザの設定を変更してください。

2.2.2 管理用のユーザーIDの設定

管理用のユーザーIDは、Appliance Managerとデータベースの管理で使用します。
“付録I デザインシート”の“表I.3 ユーザーID”で決めたAppliance Manager設定の管理用のユーザーIDとパスワードを入力し、[次へ]ボタンをクリックします。
パスワードを忘れるとHA Database Readyの運用ができなくなりますので、パスワードは忘れないようにしてください。

2.2.3 業務ネットワーク、内部ネットワーク設定

業務ネットワーク、内部ネットワークを設定します。



1. 業務ネットワークと接続するために、[IPv4アドレスを使用する]および[IPv6アドレスを使用する]の、どちらかまたは両方をチェックし、業務用のIPアドレスを設定します。IPv4とIPv6の両方の形式のIPアドレスを同時に指定できます。

設定項目(IPv4の場合)	“付録I デザインシート”の“表I.1 IPアドレス”の項番	マニュアルの説明で使用する値
[IP1]	(1)	*172.20.10.10*
[IP2]	(2)	*172.20.10.11*
[Netmask]	(3)	*255.255.255.0*
[Gateway]	(4)	*172.20.10.1*

設定項目(IPv6の場合)	“付録I デザインシート”の“表I.1 IPアドレス”の項番	マニュアルの説明で使用する値
[IP1]	(5)	－
[IP2]	(6)	－
[Prefix Size]	(7)	－
[Gateway]	(8)	－

ポイント

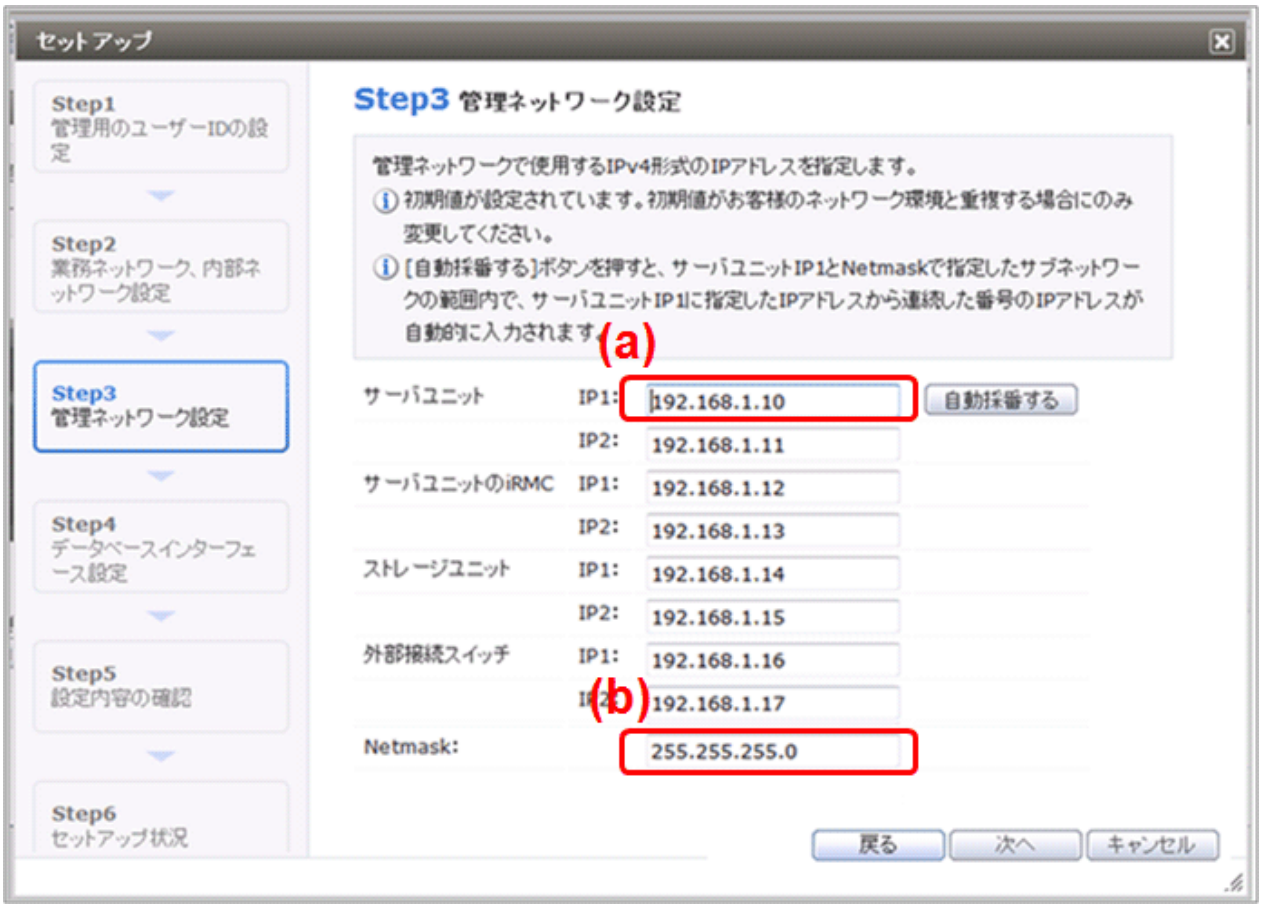
- このIPアドレスは、アプリケーションからデータベースへのアクセスに使用します。管理者から業務開発者に値を連絡してください。
- IPv6形式のIPアドレスには、グローバルユニキャストアドレスだけが指定可能です。

2. [内部ネットワークで使用するIPアドレス(IPv4形式)]に、内部ネットワークで使用するIPv4形式のIPアドレス(“付録I デザインシート”の“表I.1 IPアドレス”(9) (*192.168.2.**))を設定し、[次へ]ボタンをクリックします。

2.2.4 管理ネットワーク設定

管理ネットワークを設定します。

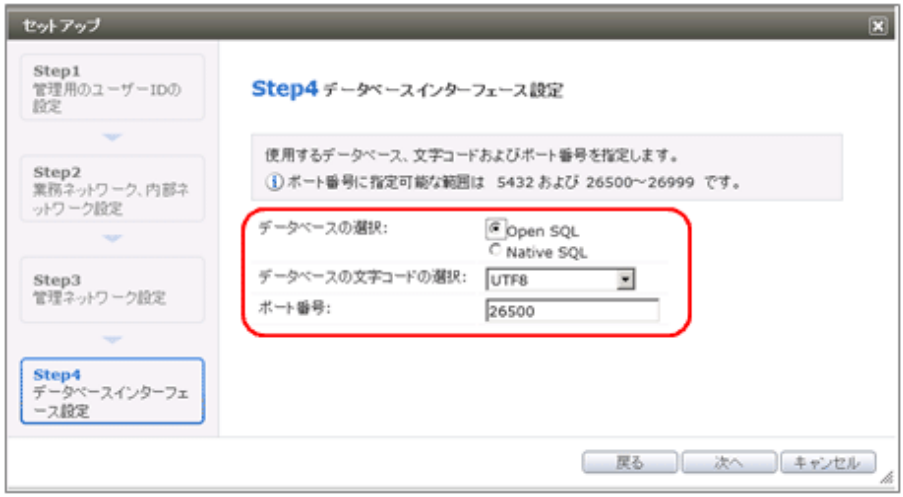
1. 管理ネットワークで使用するIPv4形式のIPアドレスを指定します。
(a)と(b)に以下に示す値を設定し、[自動採番する]ボタンをクリックしてください。[サーバユニット IP2]以降は連番で入力されます。
   - (a) : “付録I デザインシート”の“表I.1 IPアドレス”(10) (*192.168.1.10*)
   - (b) : “付録I デザインシート”の“表I.1 IPアドレス”(18) (*255.255.255.0*)



2. [次へ]ボタンをクリックします。

2.2.5 データベースインターフェース設定

データベースインターフェースを設定します。“付録I デザインシート”の“表I.2 データベース”で決めた値を指定してください。



1. [データベースの選択]で、HA Database Readyで使用するデータベースインターフェースを選択します。
   [Open SQL]または[Native SQL]の、どちらかを選択してください。
2. [データベースの文字コードの選択]で、データベースに格納する文字列型のデータの文字コードを選択します。

   [ポート番号]で、ポート番号を指定します。ポート番号に指定可能な値は、5432および26500～26999です。初期値は以下です。

   - Open SQLインターフェースの場合 ：26500
   - Native SQLインターフェースの場合：26551
3. [次へ]ボタンをクリックします。

ポイント

文字コードの選択では、アプリケーションで使用する文字コードに合わせることを推奨します。指定可能な文字コードについては、“付録C 使用可能な文字コード一覧”を参照してください。

注意

- データベースインターフェースとポート番号は、セットアップ完了後に変更できません。“D.2 データベースインターフェースの初期化”でデータベースを初期化すると再設定できます。
- セットアップ完了後は、データベースの文字コードを変更できません。“D.2 データベースインターフェースの初期化”でデータベースを初期化すると再設定できます。

2.2.6 設定内容の確認

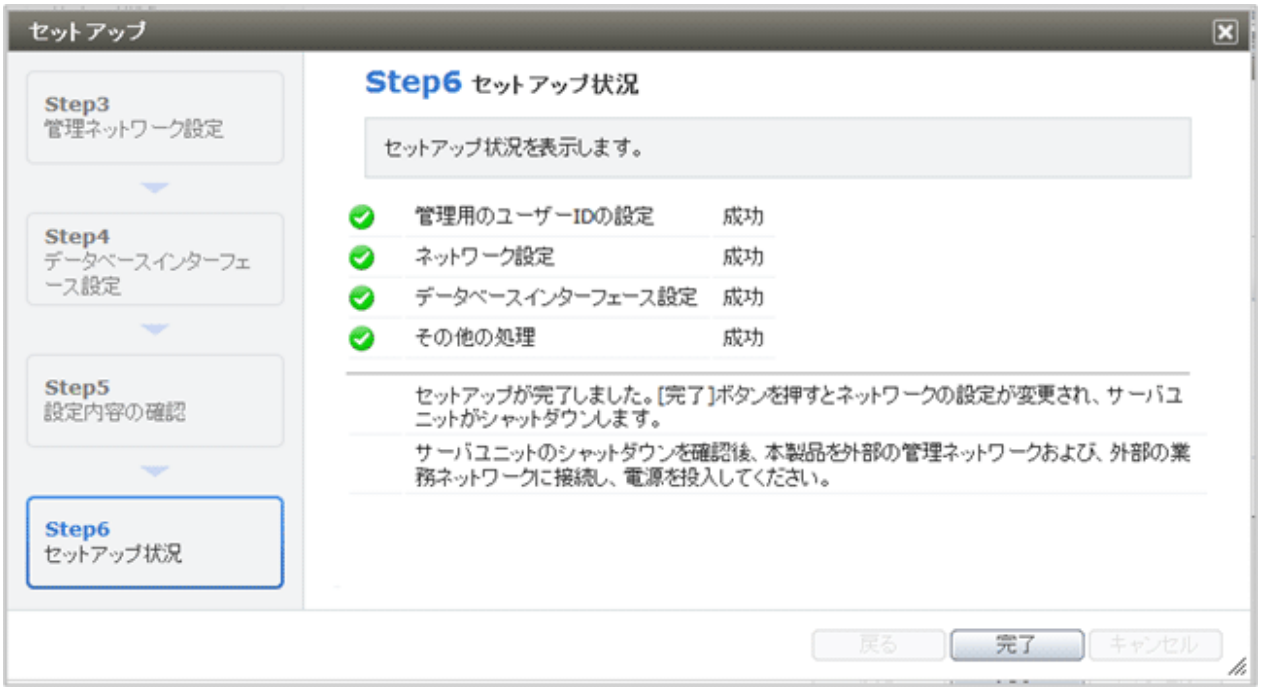
設定した内容を確認します。
内容に誤りがなければ、[セットアップ]ボタンをクリックします。
セットアップ所要時間は、“2.2.5 データベースインターフェース設定”で選択したデータベースによって異なります。セットアップ処理中は、Webブラウザの操作はできません。

- Open SQLインターフェースを選択した場合: 約5分
- Native SQLインターフェースを選択した場合: 約30分

セットアップ内容を変更する場合は、[戻る]ボタンをクリックします。

2.2.7　セットアップの完了

HA Database Readyのセットアップが完了すると、終了メッセージが表示されます。

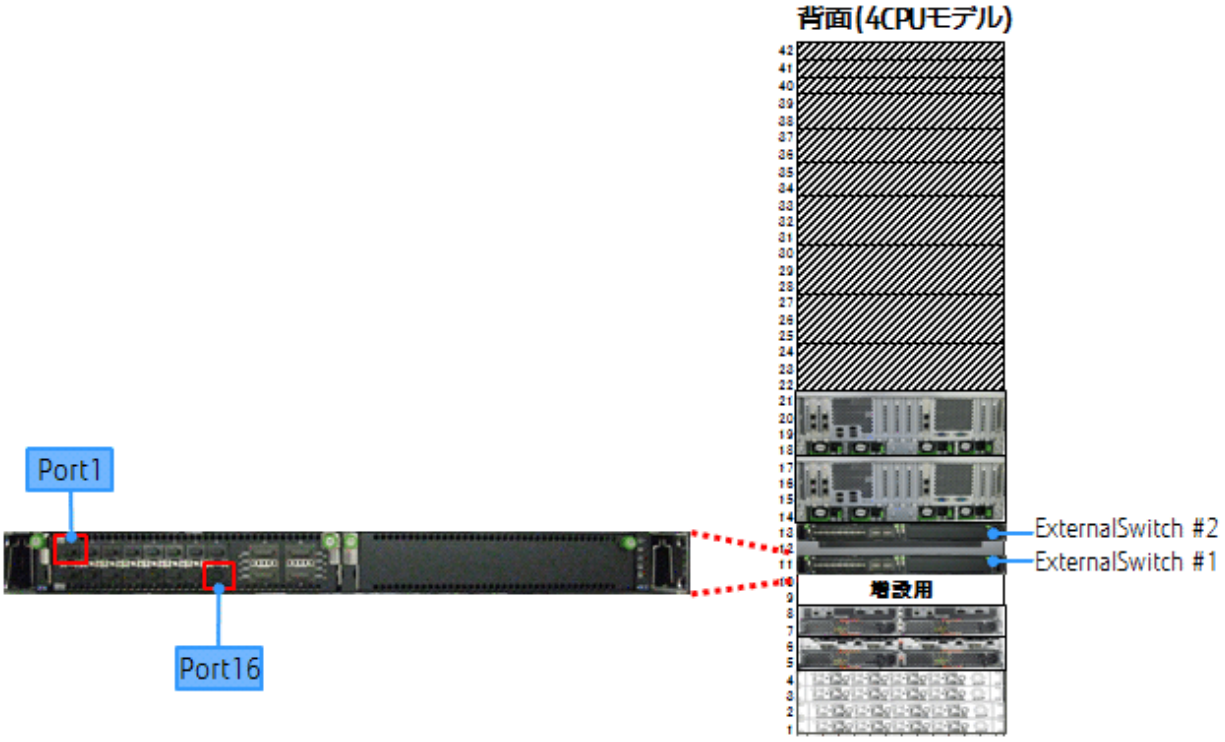


表示内容を確認したら、[完了]ボタンをクリックします。
ネットワークの設定が変更され、ServerUnit#1およびServerUnit#2がシャットダウンします。
シャットダウンが完了するまで、約12分かかります。なお、StorageUnitはシャットダウンしませんが、そのまま“2.3 外部ネットワークとの接続”に進んでください。

2.3　外部ネットワークとの接続

HA Database Readyを外部ネットワークに接続します。
接続に必要なケーブルについては、“設置ガイド”の“外部ネットワーク接続”を参照してください。

図2.2 接続するPort



1. セットアップ用PCをExternalSwitch#1のPort1から外します。
2. HA Database Readyを管理ネットワークに接続します。
   ExternalSwitch#1のPort1とExternalSwitch#2のPort1を、管理ネットワーク用お客様スイッチに接続します。
3. HA Database Readyを業務ネットワークに接続します。

   ExternalSwitch#1のPort16とExternalSwitch#2のPort16を、業務ネットワーク用お客様スイッチに接続します。
4. HA Database Readyの電源を投入します。
   電源の投入方法については、“2.1.3 電源の投入”を参照してください。

ポイント

HA Database Readyの電源投入後に、セットアップ内容の確認を行うことができます。セットアップ内容を確認する場合は、“D.1 データベースインターフェースとIPアドレスの確認”を参照してください。

参考

各アプリケーションサーバにHA Database Readyのクライアント機能をインストールする必要があります。

第3章 運用

本章では、HA Database Readyの運用について説明します。

3.1 管理端末の設定

管理端末では、Appliance Managerを利用します。また、ハードウェア故障箇所の詳細な情報の確認のため、ServerViewコンソールを利用します。用意する端末の条件について“B.1 端末の条件”を参照してください。
Appliance ManagerとServerViewコンソールを利用するために、以下の設定を実施してください。

Webブラウザの設定

管理端末のWebブラウザの設定については、“B.2 Webブラウザの設定”を参照してください。

名前解決

管理端末でServerUnit#1、ServerUnit#2の名前解決ができるようhostsファイルまたはDNSが設定されている必要があります。
ServerUnit#1のホスト名は「aphost1」、ServerUnit#2のホスト名は「aphost2」です。

hostsファイルの名前解決の設定方法は以下のとおりです。
管理端末の“C:¥Windows¥System32¥drivers¥etc¥”にあるhostsファイルに以下の例のような記述を追加します。

```
IPアドレス(注1) aphost1(注2)
IPアドレス(注1) aphost2(注2)
```

注1)aphost1とaphost2の管理用のIPアドレス(“2.2.4 管理ネットワーク設定”で[サーバユニット IP1]と [サーバユニット IP2]に指定したIPアドレス)を指定してください。
注2)“D.7 ホスト名の変更”の手順に従いホスト名を変更した場合は、新しいホスト名を指定してください。

JREのインストール

Oracle JRE 7（Java Runtime Environment 7）をインストールする必要があります。JREのバージョンは、1.7.0_40以降を使用し、OSが64bit版/32bit版に関わらず、32bit版のJREをインストールしてください。
「Javaが、セキュリティー問題の発生が考えられるアプリケーションコンポーネントを発見しました。」のメッセージが表示されないようにするには、JREをインストールした後、Java のコントロール・パネルでセキュリティの設定を変更します。
以下は、32bit版のWindows 7の例です。

1. [スタート]メニューの[コントロールパネル]をクリックします。
2. [コントロールパネルの検索]に、「Java Control Panel」と入力し、Javaのアイコンをクリックして、Javaコントロール・パネルを開きます。
3. Javaコントロール・パネルで、[詳細]タブを選択します。
4. [混合コード(サンドボックス内実行 vs. 信頼済み)セキュリティー検証]で、[有効 - 警告を表示せずに、保護をかけて実行する]をチェックします。
5. [JavaPlug-in]で、[次世代のJavaPlug-inを有効にする]をチェックします。

参考

ServerViewコンソールについては、“ServerView Suite ServerView Operations Manager V6.21 Server Management 取扱説明書”の“ServerView Operations Managerの使用”を参照してください。

管理ネットワークの経路設定

管理ネットワーク内に、ルータなどのゲートウェイを設定し、管理端末がある異なるサブネットのネットワークを接続する場合は、“D.4 管理ネットワークの経路設定”で経路を設定してください。
管理端末が、管理ネットワークと同じサブネットの場合は、経路の設定は不要です。

3.2 Appliance Managerへのログイン

HA Database Readyの運用と保守は、Appliance Managerで行います。

Appliance Managerの[ホーム]画面から、運用と保守の各操作ができます。以下の手順で、Appliance Managerにログインしてください。

1. 管理端末で、Webブラウザを起動します。
2. Webブラウザのアドレスバーに、以下のURLを入力します。

```
https://管理用のIPアドレス(注)/appmgr/
```

注)“2.2.4 管理ネットワーク設定”で[サーバユニット IP1]に指定したIPアドレスを指定してください。

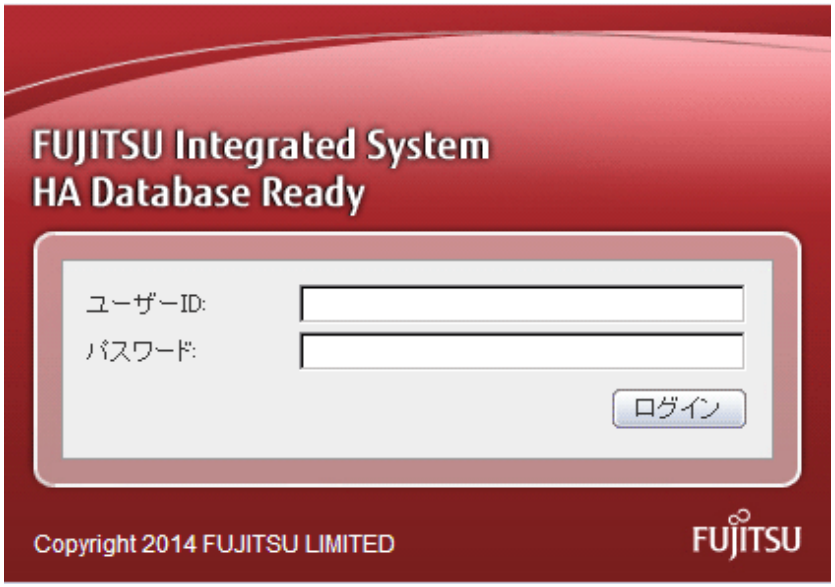
ポイント

- 誤って[サーバユニット IP2]のIPアドレスを指定した場合、正常運用時は[サーバユニット IP1] のIPアドレスにリダイレクトされます。
- ServerUnit#1が保守作業により停止している場合は、[サーバユニット IP1]に指定したIPアドレスを指定しても接続エラーになります。そのときは、[サーバユニット IP2]のIPアドレスを指定してください。

「このWebサイトのセキュリティ証明書には問題があります。」という警告が表示されますが、[このサイトの閲覧を続行する]を選択し、ログインを続行してください。この警告は、通信内容の暗号化をhttpsのプロトコルで実現するために自己署名証明書をインストールしているため発生しますが、管理端末とHA Database Readyが接続する管理ネットワークはイントラネット内に構築されるため、セキュリティ上の問題はありません。

Webブラウザに[ログイン]画面が表示されない場合や、接続中にサーバとの通信異常のエラーが発生した場合、[サーバユニット IP1]のIPアドレスのサーバが故障などにより停止していることが考えられます。その場合は[サーバユニット IP2]のIPアドレスを指定してください。

Appliance Managerの[ログイン]画面が表示されます。



参考

ー ログイン画面が表示されない場合は、“D.4 管理ネットワークの経路設定”がされているか確認してください。

3. ユーザーIDとパスワードを入力し、[ログイン]ボタンをクリックします。
   Appliance Managerの[ホーム]画面が表示されます。
   ユーザーIDとパスワードは、“2.2.2 管理用のユーザーIDの設定”で作成した管理用のユーザーIDを使用してください。

参照

Webブラウザ上でAppliance Managerの表示が崩れる場合、またはセキュリティのエラーメッセージが表示される場合は、“B.2 Webブラウザの設定”を参照して、Webブラウザ設定を変更してください。

注意

一定時間(約30分)ブラウザを操作しなかった場合、タイムアウトとなり、次の操作でログイン画面に戻ります。

3.3 運用監視

Appliance Managerにログインすると、[ホーム]画面が表示されます。[ホーム]画面では、HA Database Readyの稼働状態を確認できます。

注意

ログインするとWebブラウザのURLに“index.jsp”が付加されて“https://*管理用のIPアドレス*/appmgr/index.jsp”と表示されますが、ログインする時にはURLに“index.jsp”を指定しないでください。指定した場合、サーバの状態が誤って判断されて、機能制限された状態でログインする場合があります。
URLに“index.jsp”を指定してログインした場合は、ログアウトし、“index.jsp”なしのURLで再度ログインしてください。
以下に、機能制限された状態の[ホーム]画面例を示します。

稼働状態

HA Database Readyの状態をアイコンと文字で表示します。
稼働状態の表示と意味について、以下に示します。

表3.1 稼働状態の表示の意味と説明

状態	意味	説明	稼働状態	対処
稼働状態：正常	正常	問題なくデータベースサービスが稼働している状態です。	問題なく運用されています。	必要ありません。
稼働状態：警告	警告	データベースサービスは継続利用可能ですが、何らかの問題が発生している状態です。	以下のいずれかの状態です。 ・ 二重化したデータベースの一方が停止している ・ データベースは運用できているが、ハードウェアに何らかの異常、または警告が発生している ・ データベースは運用できているが、バックアップに失敗している	対処ウィンドウに対処方法が表示されますので、説明に従って対処してください。 詳細については、“3.4 警告・異常時の対処とリカバリー”を参照してください。
稼働状態：異常	異常	データベースサービスが継続利用不可能なエラーが発生して、データベースサービスが停止している状態です。	二重化したデータベースの両方が停止しています。	

備考. 以下の場合に、機器の異常以外で一時的に稼働状態が「異常」を示すことがあります。この場合、1分程度で「正常」に戻ります。
・リカバリーのためにシステムが自動的にデータベースを停止した

リカバリーボタン

リカバリーボタンは、HA Database Readyの異常が発生した後にデータベースを最新の状態に復旧するために使用します。リカバリーの詳細は、“3.4 警告・異常時の対処とリカバリー”を参照してください。

[自動更新を有効にする]

チェックボックスが有効の状態で表示されます。
チェックボックスを有効にすると、[ホーム]画面の各項目の表示を30秒おきに自動的に最新化します。
チェックボックスを有効にした場合、画面が定期的に更新されるため、ブラウザを操作しない状態が続いてもタイムアウトしません。画面を接続したまま放置しないようにするか、パスワード付きのスクリーンセーバーを設定して、他の人が操作できないようにしてください。
[ホーム]画面を再度開いた場合、以前のチェックボックスの状態に関わらず再びチェックボックスは有効になります。

[最新情報に更新]ボタン

[最新情報に更新]ボタンは、[ホーム]画面の稼働状態の表示を最新化するために使用します。情報の更新中は、ブラウザの操作はできません。

注意

Appliance Managerでは、ブラウザの機能による最新情報への更新([F5]キーを押すなど)を行わないでください。

メッセージウィンドウ

メッセージウィンドウには、HA Database Readyの状態を示す以下のメッセージが表示されます。表示されるメッセージの数は最大1000件です。1000件を超えた場合、古いものから削除されます。なお、1分以内に発生した同一のメッセージは、最初のメッセージだけが表示されます。

参照

メッセージは、以下の形式でAppliance Managerの[ホーム]画面のメッセージウィンドウに出力されます。

```
日付△時刻△ラベル:△エラー種別:△メッセージID: メッセージ本文
```

△は半角空白

- ラベル：“FIS-HADBR_AMGRDB”または“FIS-HADBR_AMGRCME”という文字列です。
- エラー種別：以下のエラー種別のうち1つが表示されます。

エラー種別	エラーレベル
INFO	情報(正常な状態です)
WARNING	警告
ERROR	エラー

- メッセージID：5桁の半角の数字からなる文字列が表示されます。
- メッセージ出力の例

```
2013/10/01 11:22:33 FIS-HADBR_AMGRDB: ERROR: 11002: データベースサービスが停止しました。
```

表示されるメッセージの一覧については、“付録A メッセージ一覧”を参照してください。なお、ラベルの位置に“ServerView”と表示されるメッセージは、ハードウェアに関するメッセージです。

対処ウィンドウ

対処ウィンドウには、HA Database Readyで警告または異常が発生した場合の対処方法が表示されます。警告または異常の発生時は、対処ウィンドウに表示された対処にしたがって対処を実施した後に、リカバリーボタンを押してください。

ー 対処ウィンドウの出力の例

```
FIS-HADBR_AMGRDB: ERROR: 11001
ハードウェア故障のメッセージが出力されている場合は、ハードウェア部品の交換を行ってください。
ハードウェア故障のメッセージが出力されていない場合は、初期調査資料を採取し、富士通の保守員の指示に従ってください。
・・・
```

画面右上にある以下のリンクは、Appliance Managerのすべての画面に共通です。

[ログアウト]

Appliance Managerをログアウトした後、再度ログイン画面を表示します。

[ServerViewコンソール]

ServerView Operations Managerの[ServerViewコンソール]画面が表示されます。
ServerView Operations Managerでは、以下の装置について装置上の表記と異なった表記が表示されます。

ServerViewの表記	装置上の表記
ServerUnit1	ServerUnit#1
ServerUnit2	ServerUnit#2
ExternalSwitch1	ExternalSwitch#1
ExternalSwitch2	ExternalSwitch#2

ServerViewコンソールには、Appliance Managerの管理用ユーザーIDを表すhadbrというユーザー名で自動的にログインされます。
ServerViewコンソールをログアウトした場合は、ServerViewのウィンドウをすべて閉じてください。[ServerViewコンソール]画面を表示する場合は、必ず、この[ServerViewコンソール]リンクから行ってください。

注意

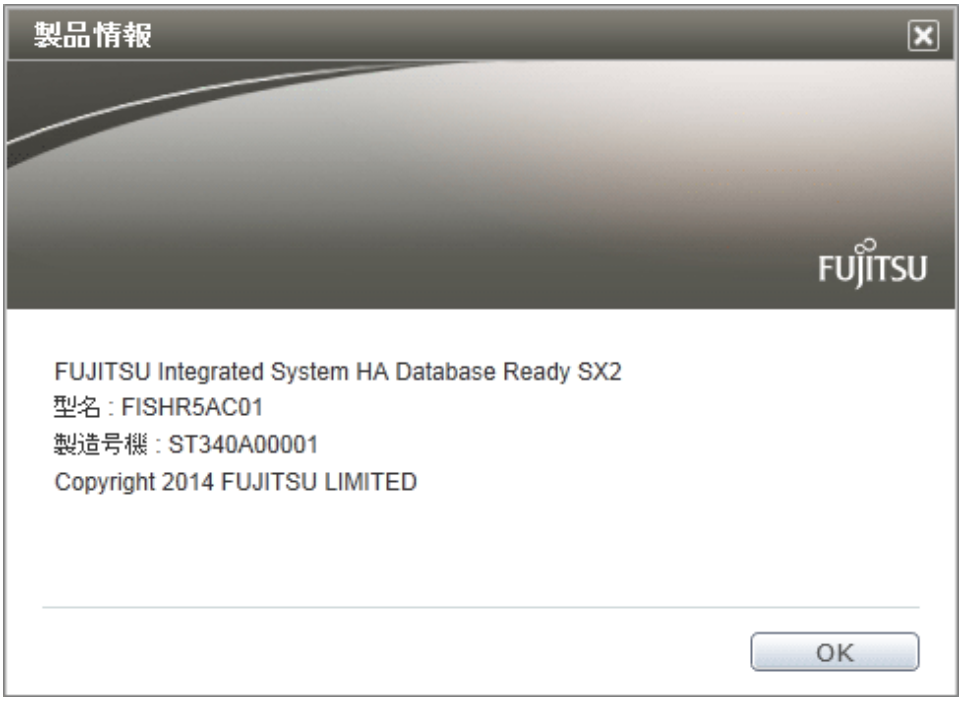
- ServerView Operations Managerで、Appliance Managerの管理用ユーザーID(hadbr)のパスワードは変更しないでください。Appliance Managerから、ServerView Operations Managerの[ServerViewコンソール]に自動的にログインできなくなります。
- リンクをクリックして表示されるウィンドウに「このWebサイトのセキュリティ証明書には問題があります。」という警告が表示されますが、[このサイトの閲覧を続行する]リンクを選択し、ログインを続行してください。
- 「このアプリケーションを実行しますか。」という警告が表示された場合、[実行]を選択してください。次回から確認が不要な場合は[この発行者および前述の場所からのアプリケーションでは、次回から表示しない]をチェックしてください。
- 「Javaが、セキュリティー問題の発生が考えられるアプリケーションコンポーネントを発見しました。」という警告が表示された場合は、[いいえ]を選択してください。メッセージが表示されないようにするには、“3.1 管理端末の設定”の“JREのインストール”のセキュリティの設定を行ってください。
- 「このWebサイトから次のアプリケーションへのアクセスを許可しますか。」という警告が表示された場合、[許可する]を選択してください。
- 「続行しますか。このWebサイトへの接続は信頼できません。」という警告が表示された場合、[続行]を選択してください。
- ServerView Operations Manager画面でStorageUnitを選択した場合、ストレージ情報画面が正常に表示されないときがあります。
  この場合は、ストレージ情報画面を閉じ、再度StorageUnitを選択してください。

[マニュアル]

HA Database Readyのオンラインマニュアルを開きます。
「このWebサイトのセキュリティ証明書には問題があります。」という警告が表示されますが、[このサイトの閲覧を続行する]リンクを選択し、ログインを続行してください。

[製品情報]

[製品情報]ウィンドウが表示されます。



HA Database Readyの型名と製造号機を表示します。

ポイント

- 本ウィンドウの情報(型名と製造号機)で、お使いのHA Database Readyのハードウェア構成が特定できます。この情報は、トラブル発生時に弊社保守員へ連絡する場合に必要となります。
- 対象製品の型名情報については、“設置ガイド”を参照ください。

参考

Appliance Managerの[ホーム]画面で監視するほかに、データベース稼働状態やハードウェアの状態は、以下の方法で監視することができます。

- 外部に設置された運用管理サーバで監視する。
- 稼働状態をメールで受け取る。

詳細は、“付録E 運用管理サーバとの連携”の“E.1 運用監視”および“E.3 メール通知”を参照してください。

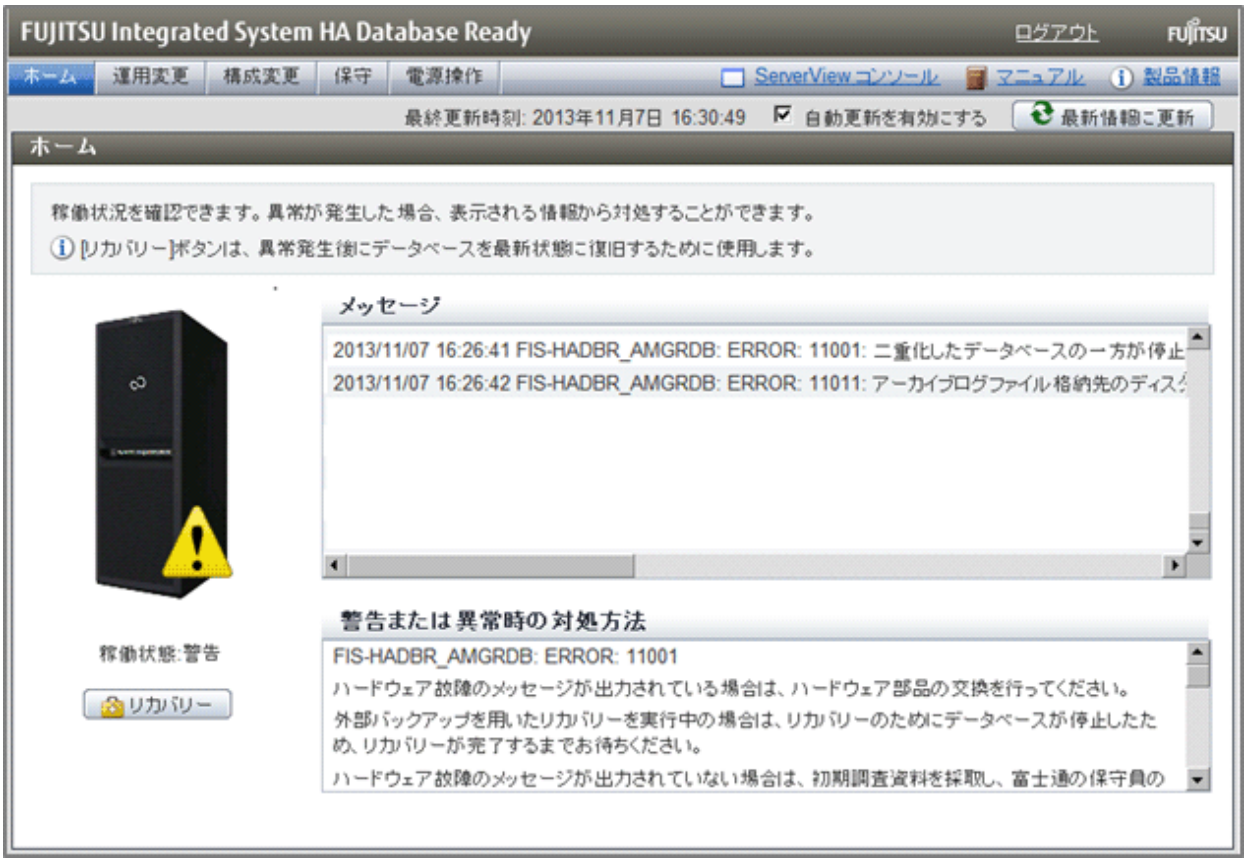
3.4 警告・異常時の対処とリカバリー

ここでは、[ホーム]画面の稼働状態に「警告」や「異常」が表示された場合の対処方法について説明します。

対処とリカバリー

HA Database Readyに何らかの異常が発生した場合、Appliance Managerの[ホーム]画面の対処ウィンドウとメッセージウィンドウに対処方法とメッセージが表示されます。表示されるメッセージの詳細については、“付録A メッセージ一覧”を参照してください。

以下の手順で対処してください。



1. [ホーム]画面の稼働状態が「警告」や「異常」を示している場合は、対処ウィンドウに表示されている対処方法に従って、対処してください。
   機能制限された状態でログインしている場合は、対処完了後にログアウトし再度ログインすることで機能制限がなくなります。手順2以降の操作は機能制限なしの状態で実施してください。

   ポイント

   対処ウィンドウに以下の内容が表示された場合は、ハードウェアに何らかの異常、または警告が発生しています。
   SupportDesk契約に基づいて、富士通のサポートセンターに連絡して故障箇所を特定してください。
   ハードウェア部品の交換が必要な場合は、“3.6.4 ハードウェア部品交換”の手順を実施してください。ハードウェア部品の交換が終了した後に、手順2.を実施してください。
   ハードウェアの故障でない場合は、手順2.に進み、リカバリーボタンをクリックして警告状態を解除してください。

   ー「ハードウェアの異常を検出しました。富士通の保守員に連絡して、故障部品を交換してください。」

2. 対処ウィンドウに表示されている、リカバリー処理に必要な時間、リカバリー中の注意事項、制限事項を確認してください。必要に応じて、アプリケーションの停止や、利用者へ停止をアナウンスしてください。
3. 対処ウィンドウの注意事項を確認したら、リカバリーを実行してデータベースを最新の状態に復旧します。

   リカバリーは、Appliance Managerで以下の手順で実施します。

注意

Native SQLインターフェースを選択した場合、リカバリー開始後にデータベースサービスが停止します。停止時間の詳細については、“表3.2 リカバリー所要時間の目安”を参照してください。

a. Appliance Managerにログインして、[ホーム]画面を開きます。[ホーム]画面のリカバリーボタンをクリックしてください。確認画面が表示されるので、[OK]をクリックしてください。

b. リカバリーを開始すると、メッセージウィンドウにリカバリーの開始メッセージが表示されます。リカバリーが完了すると、リカバリーの完了メッセージが表示され、画面上の稼働状態が「正常」に変わります。

参考

データベースを復旧する必要が無い、または最初からデータベースを作成しなおしたい場合には、HA Database Readyのデータベースインターフェースを初期化して、復旧する方法もあります。初期化の詳細については、“D.2 データベースインターフェースの初期化”を参照してください。これにより、ホーム画面の稼働状態が「正常」に変わります。

4. リカバリーの結果は、メッセージウィンドウに表示されます。
メッセージウィンドウの内容を確認して、アプリケーションの再開や、利用者へ再開をアナウンスしてください。
また、警告や異常の原因がハードウェアの場合は、サーバの保守ランプ(エラーランプ)の点灯・点滅を解除してください。保守ランプの点灯・点滅の解除については、“3.6.7 保守ランプについて”を参照してください。

注意

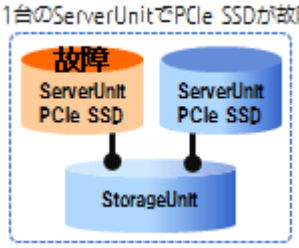
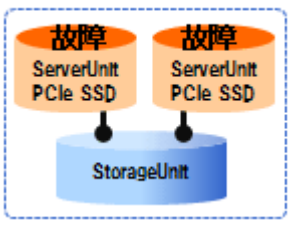
- 警告や異常の原因となったハードウェアの修理が完了していないときにリカバリーボタンをクリックすると、リカバリー処理が失敗します。必ずハードウェアの修理が完了してからリカバリーボタンをクリックしてください。
- リカバリー処理中は、Appliance Managerの画面操作を行うことができます。また、Appliance Managerからログアウトしても、リカバリー処理は継続します。
- リカバリーが完了すると、データベースは最新の状態に復旧されます。

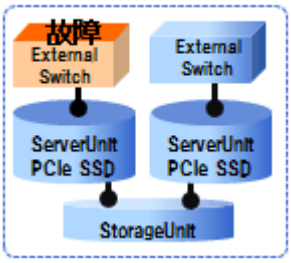
参考

- ハードウェアの故障を検出した場合、故障した箇所の詳細な情報はServerView Operations Managerで確認してください。
  - ー ServerView Operations Managerを起動するには、Appliance Managerの画面右上の[ServerViewコンソール]リンクをクリックしてください。なお、ServerView Operations Managerを利用するには、管理端末で、ServerUnit#1、ServerUnit#2の名前解決ができるよう設定することと、JREのインストールが必要です(“3.1 管理端末の設定”参照)。
  - ー ServerView Operations Managerについては、“ServerView Suite ServerView Operations Manager V6.21 Server Management 取扱説明書”の“ServerView Operations Managerの使用”を参照してください。
- HA Database Readyでは最適な設定をしておりますので、お客様がストレージの設定を変更する必要がありません。そのため、[RAID Manager]へのリンクおよび[ストレージGUI]へのリンクは使用できません。

HA Database Readyで異常が発生した場合のリカバリー方法と、リカバリー所要時間の目安、操作制限について、以下の表に示します。なお、以下の表ではリカバリーボタンで復旧できる例について説明しています。

表3.2 リカバリー所要時間の目安

異常発生箇所	管理者の操作制限		リカバリー方法	リカバリー所要時間の目安(注1)			業務停止時間	
	異常発生中	リカバリー中(注2)		モデル(注3)	Open SQL	Native SQL	Open SQL	Native SQL
	・運用変更操作 ・データベースの定義変更(注4)	・運用変更操作 ・バックアップ ・データベースの定義変更(注4)	(1)ハードウェア修理 (2)電源投入 (3)リカバリーボタンのクリック	2CPU	2時間	6時間	停止せず	リカバリー開始後約7分
				2CPU＋	4時間	12時間		
				4CPU	4時間	16時間		
				4CPU＋	6時間	24時間		
	・すべての運用操作	・すべての運用操作		2CPU	3時間	18時間	2時間(注5)	13時間(注5)
				2CPU＋	6時間	30時間	3時間(注5)	19時間(注5)
				4CPU	7時間	37時間	3時間(注5)	22時間(注5)
				4CPU＋	10時間	54時間	5時間(注5)	31時間(注5)

異常発生箇所	管理者の操作制限		リカバリー方法	リカバリー所要時間の目安(注1)			業務停止時間	
	異常発生中	リカバリー中(注2)		モデル(注3)	Open SQL	Native SQL	Open SQL	Native SQL
外部接続スイッチ1台が故障 	なし	なし		全モデル	1分	1分	停止せず	停止せず

注1)リカバリーの所要時間は、ハードウェアの修理が完了し、リカバリー処理を開始してからの時間です。
注2)選択したデータベースの種類によっては、リカバリー処理中に一時的に業務継続ができなくなる場合があります。この情報は、対処ウィンドウに出力されます。
注3)以下の製品のモデルを表します。詳細は“1.1.3 基本スペック”を参照してください。
・2CPU : 2CPUモデル。各ServerUnitにPCIe SSD(2.4TB)を1台搭載。
・2CPU＋: 2CPUモデルに容量増設オプションを追加した場合。各ServerUnitにPCIe SSD(2.4TB)を2台搭載。
・4CPU : 4CPUモデルです。各ServerUnitにPCIe SSD(2.4TB)を2台搭載。
・4CPU＋: 4CPUモデルに容量増設オプションを追加した場合。各ServerUnitにPCIe SSD(2.4TB)を3台搭載。
注4)Native SQLインターフェースを選択した場合だけ、データベースサービスが停止します。
注5) リカバリー開始後の業務停止時間を示します。2台のServerUnitでPCIe SSDが故障した場合のリカバリーでは、データベースの一方が復旧した時点で、業務が開始できるようになります。

注意

- 2箇所で異常が発生した状態からのリカバリーは長時間を要し、業務停止時間も長くなります。そのため1箇所で異常が発生した時点で、早急にリカバリーを実施してください。
- 冗長化されたネットワーク構成で二重障害が発生した場合、サーバは切り替わらないため、業務継続できません。片方のネットワークで異常が発生した時点で、早急にリカバリーを実施してください。

参考

- リカバリー時間の目安は、特定のデータベース構成モデルの場合です。モデルの詳細については、“表3.3 リカバリー時間の算出で想定しているデータベース規模”を参照してください。
- リカバリーの所要時間は、定義した要素の数と、バックアップを取得してからデータベースに異常が発生するまでに更新したデータ量に従って変動します。ここでは、およそ50ギガバイトが更新された時点の所要時間を記載しています。

“表3.2 リカバリー所要時間の目安”で想定しているデータベースの規模を説明します。

表3.3 リカバリー時間の算出で想定しているデータベース規模

要素	値
データベース数	1
データベースの総容量	各モデルの最大値
実表の数(注1)	8,000
インデックスの数(注2)	24,000

注1)Native SQLインターフェースを選択した場合は、“実表のDSI数”に置き換えてください。
注2)Native SQLインターフェースを選択した場合は、“インデックスのDSI数”に置き換えてください。

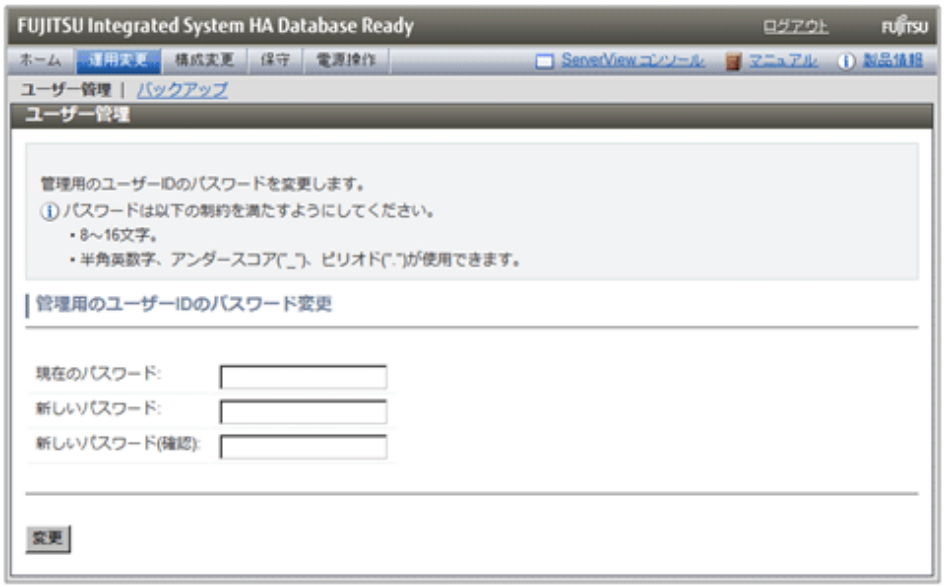
3.5 運用変更

ここでは、HA Database Readyの運用変更で必要な作業について説明します。

3.5.1 管理用のユーザーIDのパスワード変更

管理用のユーザーIDのパスワードを変更できます。

1. Appliance Managerで[運用変更]タブを選択し、次に[ユーザー管理]タブを開きます。[ユーザー管理]画面が開きます。



2. [現在のパスワード]、[新しいパスワード]、および[新しいパスワード(確認)]を入力します。
パスワードを忘れるとHA Database Readyの運用ができなくなりますので、パスワードは忘れないようにしてください。
3. [変更]ボタンをクリックします。新しいパスワードが設定されます。
以下の場合は、メッセージが表示されますので、パスワードを修正してください。
   - 変更前のパスワードに誤りがある
   - 変更後のパスワードが制約を満たしていない
   - 変更後のパスワードが一致していない

   パスワードの制約については、“2.2.2 管理用のユーザーIDの設定”を参照してください。

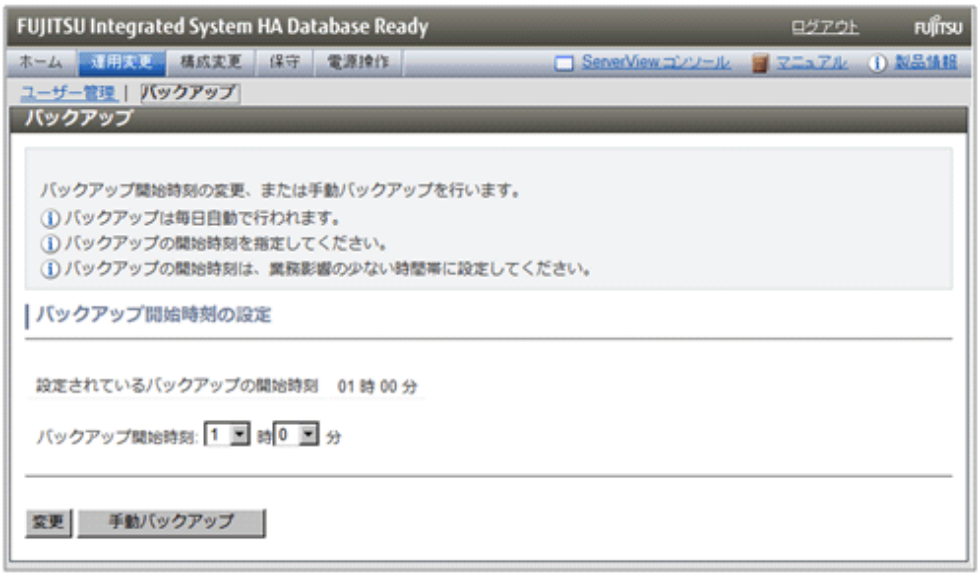
3.5.2 バックアップ

HA Database Readyは、異常発生時に備えて、データベース資源のバックアップを自動的に行います。そのバックアップとデータベースのトランザクションの記録を使用することで、HA Database Readyの一部ハードウェアに故障が発生した場合でも、システムを最新の状態まで復元できます。

バックアップは、お客様が設定した開始時刻に定期的に取得します。開始時刻を設定する場合は、業務への影響を避けるため、業務負荷が低い時間帯に設定することを推奨します。初期値は毎日午前1時に実行されるように設定されています。

この設定を変更する場合は、以下の手順で行います。

1. Appliance Managerで[運用変更]タブを選択し、次に[バックアップ]タブを開きます。[バックアップ]画面が開きます。



2. [バックアップ開始時刻]を指定します。
3. [変更]ボタンをクリックします。新しいバックアップスケジュールが設定されます。

ポイント

- [手動バックアップ]ボタンをクリックすると、[バックアップ開始時刻]に関係なく、すぐにバックアップを実施します。
- バックアップ処理中は、Appliance Managerの画面操作を行うことができます。また、Appliance Managerからログアウトしても、バックアップ処理は継続します。
- バックアップ所要時間の目安は、以下のとおりです。所要時間は、格納しているデータ量に依存します。

製品のモデル種別(注)	Open SQL	Native SQL
2CPUモデル	2時間	2時間
2CPUモデル＋容量増設オプション	4時間	5時間
4CPUモデル	4時間	6時間
4CPUモデル＋容量増設オプション	6時間	9時間

注) 各モデルの詳細は“1.1.3 基本スペック”を参照してください。

注意

- バックアップに失敗した場合は、[ホーム]画面の稼働状態の表示が「警告」になります。
- バックアップに失敗した状態を放置すると、システムの復元ができなくなる場合があります。早急に復旧してください。詳細は、“3.4 警告・異常時の対処とリカバリー”を参照してください。
- バックアップ開始時に前回のバックアップが動作中の場合、バックアップは実行されません。

3.6 保守

ここでは、HA Database Readyの修正の適用方法、修正の削除方法、初期調査資料の採取方法、ハードウェア部品交換時の運用操作、運用中の容量追加、およびBIOS/ファームウェアの更新方法を説明します。

3.6.1 修正適用

HA Database Readyは、ローリングアップデートによるソフトウェアの一括修正の適用をサポートしています。

HA Database Readyの修正の適用は、2台のサーバのそれぞれに対して行う必要があります。以下の手順で修正を適用してください。

修正のダウンロード

SupportDesk契約に基づいて弊社から通知されたサイトから、HA Database Readyの修正ファイルと修正説明書をダウンロードして管理端末に格納します。
修正ファイルは、HA Database Readyの修正ファイルで、修正説明書は、修正ファイルに含まれる修正一覧と、HA Database Readyに適用可能なRed Hat Enterprise Linuxの修正一覧などが記載されています。
修正ファイルはzip形式で圧縮されており、修正ファイル名は「AS+5桁の数字」で構成されています(例:AS12121.zip)。

1. 修正説明書をテキストエディタなどで開き、適用するRed Hat Enterprise Linuxの修正を確認してください。Red Hat Enterprise Linuxの修正が記述されている場合には、手順2.に進んでください。適用するRed Hat Enterprise Linuxの修正が記述されていない場合は、手順3.に進んでください。

   例) 修正説明書の記述例(Red Hat Enterprise Linuxの修正)

   ```
   [Red Hat Enterprise Linuxの修正]
   以下のRed Hat Enterprise Linuxの修正をダウンロードしてください。
   ----------------------------------------------------------------------------------------
   glibc-2.12-1.47.el6_2.XX.x86_64.rpm
   glibc-common-2.12-1.47.el6_2.XX.x86_64.rpm
   ----------------------------------------------------------------------------------------
   ```

2. 以下の手順で、Red Hat Enterprise Linuxの修正を修正ファイルに取り入れます。

   a. 手順1.の修正ファイルを任意のフォルダに解凍します。解凍したフォルダの下には以下のフォルダが作成されます。

   ```
   ¥修正ファイル名¥rpm¥OS¥rpm
   ```

   b. Red Hat Enterprise Linuxのサブスクリプション契約時に通知されたRedHat社のサイト「カスタマーポータル」から、修正説明書に記述されている修正だけをダウンロードして、上記フォルダに配置してください。

   参考

   RedHat社のサイト「カスタマーポータル」にアクセスするには、サブスクリプションの登録が必要です。サブスクリプションの登録については、SupportDesk契約に基づいて弊社から通知されたサイトで公開しているSupportDeskサービスご契約者様向けの「Linuxユーザーズマニュアル RHEL6編」の「6.2.1 カスタマーポータルへのサブスクリプションの登録／更新」を参照してください。

   c.「修正ファイル名」フォルダ配下のファイルを、「修正ファイル名」のフォルダごとzip形式で圧縮して、ひとつのzipファイル(パスワード無し）にしてください。また、zipのファイル名は、手順1.の修正ファイル名と同じにしてください（AS+5桁の数字.zip)。

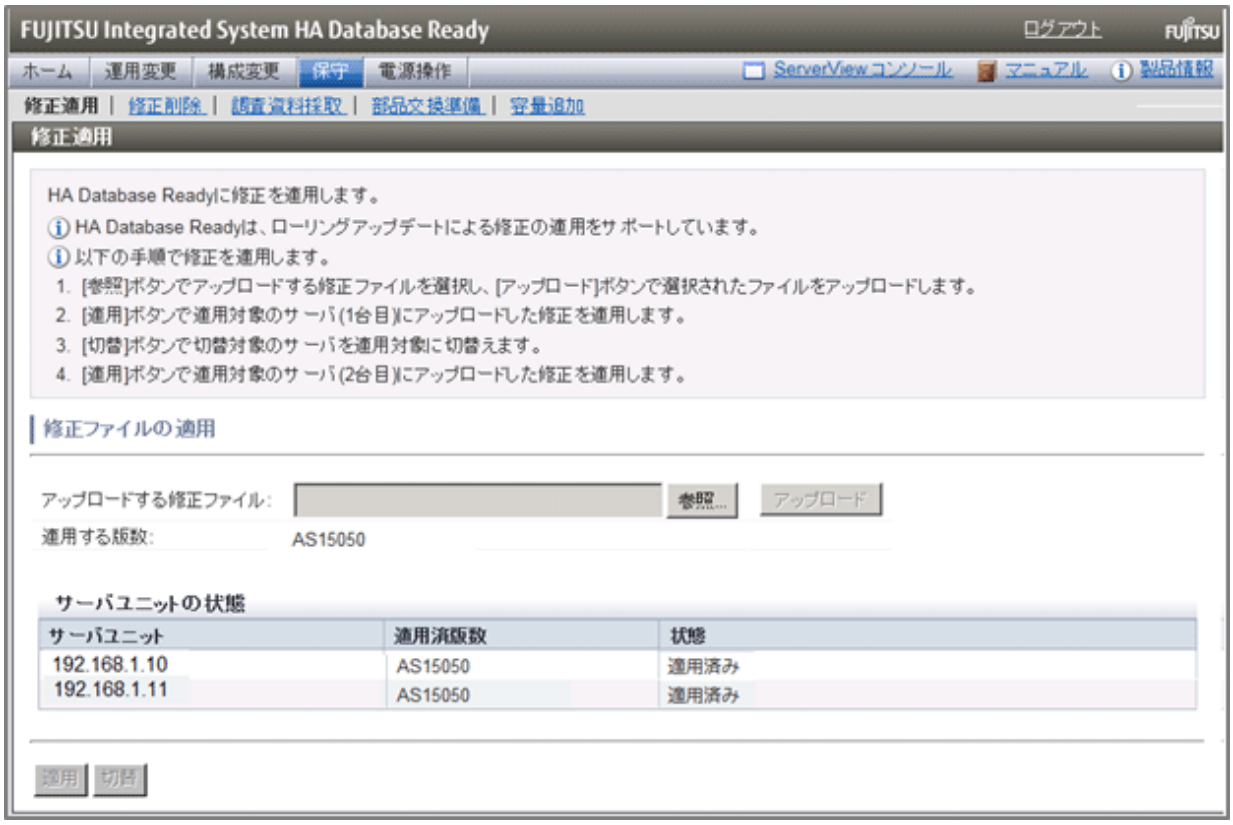
注意

Red Hat Enterprise Linuxの修正は、上記の手順に従って、RedHat社のサイト「カスタマーポータル」から修正をダウンロードし、適用してください。上記の手順以外で修正を適用しないでください。

弊社では、修正説明書に記載されているHA Database Readyの修正とRed Hat Enterprise Linuxの修正の組み合わせでの動作確認を実施しております。修正説明書に記載されていない修正をダウンロードして適用すると、動作を保証できません。

3. Appliance Managerの[ホーム]画面の稼働状態が「正常」になっていることを確認します。稼働状態が「正常」の場合にだけ、修正ファイルのアップロードや修正適用が可能です。

4. [修正適用]画面で、[参照]ボタンをクリックし、アップロードする修正ファイルとして、Red Hat Enterprise Linuxの修正を含んだ修正を作成した場合は、手順2.のc.で作成したzipファイル、そうでない場合には、手順1.でダウンロードしたzipファイルを選択します。



参考

- [適用する版数]には、選択した修正ファイルの版数が表示されます。
  修正ファイルを選択していない場合には、過去に選択した修正ファイルの版数が表示されます。
  過去に修正が適用されていない場合、稼働状態が正常でない場合、または[状態]が「適用中」と表示されている場合には、「----」が表示されます。
- [適用済版数]には、サーバに適用されている最新の修正ファイルの版数が表示されます。ただし、過去に修正が適用されていない場合や稼働状態が正常でない場合には、「----」が表示されます。
- [状態]には、以下のいずれかが表示されます。
  - 適用未：[適用する版数]に表示された修正ファイルが、適用されていない状態
  - 適用済み：[適用する版数]に表示された修正ファイルが、既に適用されている状態
  - 適用対象:[適用する版数]に表示された修正ファイルが、適用可能な状態
  - 切替対象:[切替]ボタンをクリックした場合に、本サーバの切り替えが実行されることを意味します。
  - 適用中：[適用する版数]に表示された修正ファイルを適用している状態
  - ----:過去に修正が適用されていない。もしくは、本サーバの稼働状態が正常でないことを意味します。

5. [アップロード]ボタンをクリックします。

修正適用（1台目）

1. [修正適用]画面で、[状態]に「適用対象」が表示されていることを確認し、[適用]ボタンをクリックして、1台目のサーバに修正を適用します。
2. Webブラウザを終了するよう画面に表示された場合、Webブラウザを終了し、その後Appliance Managerに再度ログインします。修正適用の所要時間は、約30分です。約30分後に、手順3.に進んでください。
3. 再度、[修正適用]画面を開き、修正を適用したサーバの[状態]が「適用済み」と表示されていることを確認してください。[状態]が「適用中」と表示された場合には、時間を空けて、再び[修正適用]画面を開いて[状態]を確認してください。

修正適用（2台目）

2台目の適用では、修正を適用するサーバを切り替えるため、データベースサービスが一時的に数秒間停止します。このため、2台目を実施する際の切替え時は、必ず業務が停止中であることを確認して実施してください。

1. [修正適用]画面で、[状態]に「切替対象」が表示されていることを確認し、[切替]ボタンをクリックします。[切替]ボタンがクリックできない場合には、時間を空けて、再び[修正適用]画面を開いて[切替]ボタンをクリックしてください。
2. [状態]に「適用対象」が表示されていることを確認し、[適用]ボタンをクリックして、2台目のサーバに修正を適用します。
3. Webブラウザを終了するよう画面に表示された場合、Webブラウザを終了し、その後Appliance Managerに再度ログインします。修正適用の所要時間は、約30分です。約30分後に、手順4.に進んでください。
4. 再度、[修正適用]画面を開き、修正を適用したサーバの[状態]が「適用済み」と表示されていることを確認してください。[状態]が「適用中」と表示された場合には、時間を空けて、再び[修正適用]画面を開いて[状態]を確認してください。

注意

修正適用を実施中に、アプリケーションによりデータベースのデータが大量に更新された場合、1台目の修正適用作業を開始してから、2台目の修正適用作業の[切替]ボタンがクリックできるようになるまで、時間がかかります。そのため、修正適用作業は、業務負荷が低い時間帯に実施してください。

3.6.2 修正削除

適用した修正に何らかの問題があり、修正を削除（バックアウト）する場合の手順を説明します。

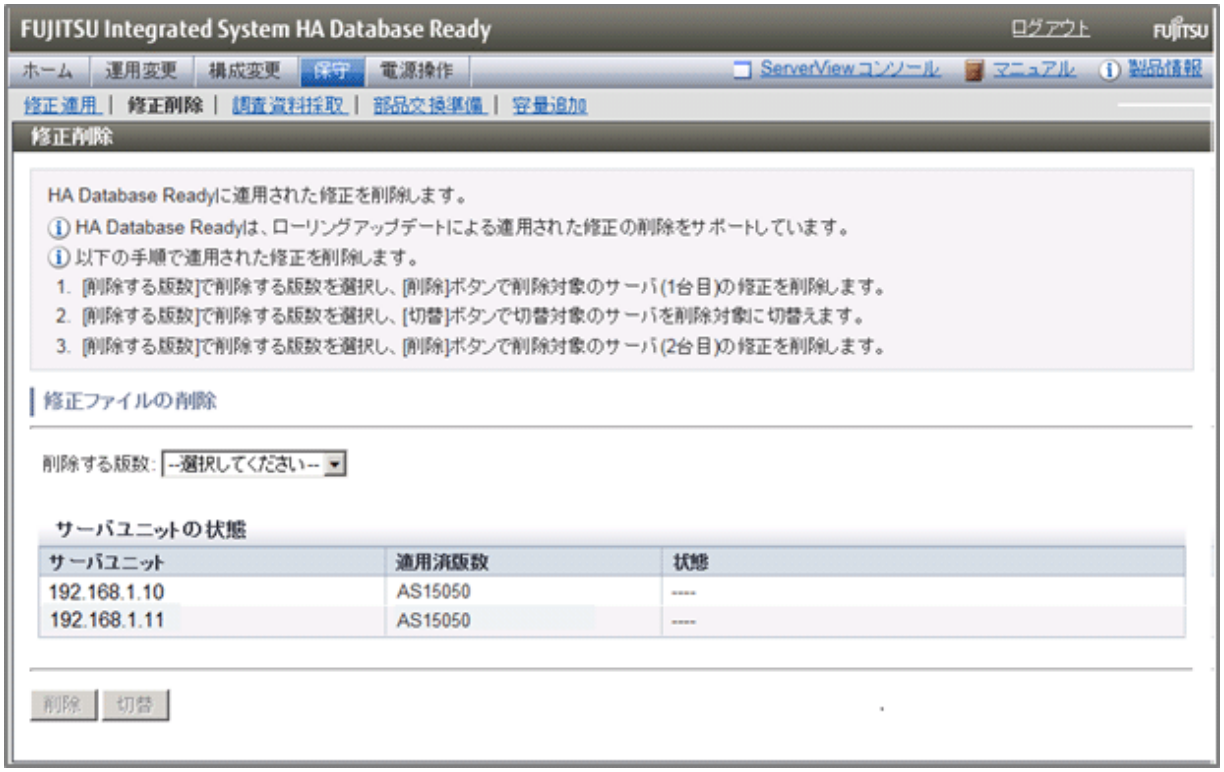
HA Database Readyは、ローリングアップデートによる修正の削除をサポートしています。

HA Database Readyの修正の削除は、2台のサーバのそれぞれに対して行う必要があります。以下の手順で修正を削除してください。

修正削除（1台目）

1. Appliance Managerの[ホーム]画面の稼働状態が「正常」になっていることを確認します。稼働状態が「正常」の場合にだけ、修正削除が可能です。

2. 1台目のサーバの場合、[修正削除]画面で削除する修正の版数を選択します。



参考

- [削除する版数]には、サーバに適用されている最新の修正ファイルの版数が表示されます。ただし、過去に修正が適用されていない場合、稼働状態が正常でない場合、または[状態]が「削除中」と表示されている場合には、「----」が表示されます。
- [状態]には、以下のいずれかが表示されます。
  - 削除未：[削除する版数]に表示された修正ファイルが、削除されていない状態
  - 削除済み：[削除する版数]に表示された修正ファイルが、既に削除されている状態
  - 削除対象：[削除する版数]に表示された修正ファイルが、削除可能な状態
  - 切替対象：[切替]ボタンをクリックした場合に、本サーバの切り替えが実行されることを意味します。
  - 削除中：[削除する版数]に表示された修正ファイルを削除している状態
  - ----：[削除する版数]が選択されていない。もしくは、本サーバが正常でないことを意味します。

3. [状態]に「削除対象」が表示されていることを確認し、[削除]ボタンをクリックして、1台目のサーバの修正を削除します。
4. Webブラウザを終了するよう画面に表示された場合、Appliance Managerを表示しているWebブラウザを終了し、その後Appliance Managerに再度ログインします。修正削除の所要時間は、約30分です。約30分後に、手順5.に進んでください。
5. 再度、[修正削除]画面を開き、[削除する版数]で削除した版数を選択し、修正を削除したサーバの[状態]が「削除済み」となっていることを確認してください。[状態]が「削除中」と表示された場合には、時間を空けて、再び[修正削除]画面を開いて[状態]を確認してください。

修正削除（2台目）

2台目の削除では、サーバを切り替えるため、データベースサービスが一時的に数秒間停止します。このため、2台目を実施する際の切替え時は、必ず業務が停止中であることを確認して実施してください。

1. [修正削除]画面で、[削除する版数]で削除する版数を選択します。[状態]に「切替対象」が表示されていることを確認し、[切替]ボタンをクリックして、修正を削除するサーバを切り替えます。[切替]ボタンがクリックできない場合には、時間を空けて、再び[修正削除]画面を開いて[切替]ボタンをクリックしてください。
2. [削除する版数]で削除する版数を選択します。[状態]に「削除対象」が表示されていることを確認し、[削除]ボタンをクリックして、2台目のサーバの修正を削除します。
3. Webブラウザを終了するよう画面に表示された場合、ブラウザを終了し、その後Appliance Managerに再度ログインします。修正削除の所要時間は、約30分です。約30分後に、手順4.に進んでください。
4. 再度、[修正削除]画面を開き、以下のいずれかであることを確認します。[状態]が「削除中」と表示されている場合には、時間を空けて、再び[修正削除]画面を開いて、以下のいずれかが表示されていることを確認してください。

   ー「適用されている修正はありません。」のメッセージが出力されている

   ー [削除する版数]で修正の版数が選択できる

注意

- 上記の修正削除の手順では、Red Hat Enterprise Linuxの修正は、削除することができません。Red Hat Enterprise Linuxの修正で問題が発生した場合には、“3.6.1 修正適用”の手順に従って、問題が解決されたRed Hat Enterprise Linuxの修正を含んだ修正ファイルを作成し、適用してください。
- 修正削除を実施中に、アプリケーションによりデータベースのデータが大量に更新された場合、1台目の修正削除作業を開始してから、2台目の修正削除作業の[切替]ボタンがクリックできるようになるまで、時間がかかります。そのため、修正削除作業は、業務負荷が低い時間帯に実施してください。

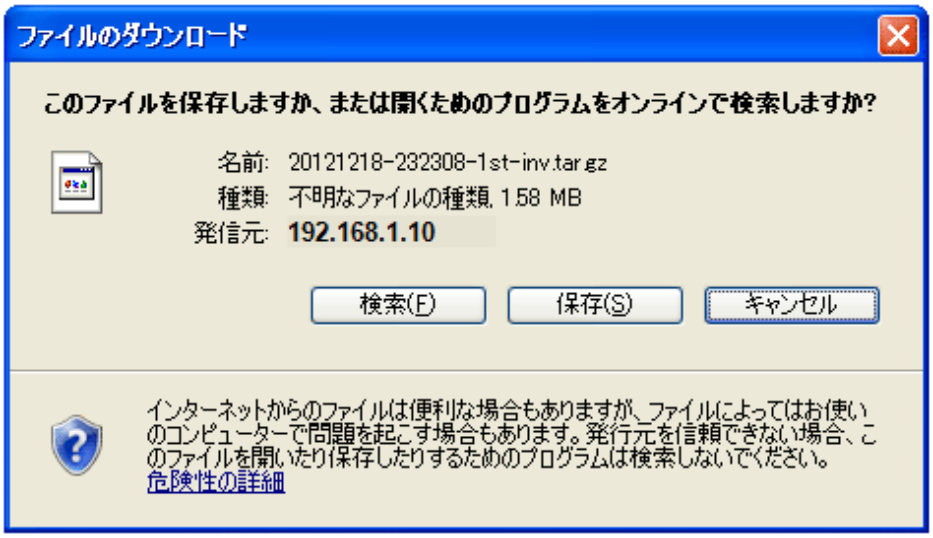
3.6.3 調査資料の採取

HA Database Readyでトラブルが発生した場合に、富士通サポートセンターに調査を依頼するときに必要となる初期調査資料の採取手順を説明します。

1. Appliance Managerで[保守]タブを選択し、次に[調査資料採取]タブを開きます。[調査資料採取]画面が開きます。

2. [採取]ボタンをクリックします。

3. サーバでの資料採取が完了すると、[ファイルのダウンロード]画面が表示されるので、ダウンロード先を指定します。



4. 手順3.で指定したダウンロード先に保存された調査資料を富士通サポートセンターへ送付してください。

ポイント

初期調査資料は、fjsnap_summaryコマンドを使用して、ディスクやプロセスの状態、定義情報などを採取しています。調査資料にお客様のユーザーデータは含まれません。
fjsnap_summaryコマンドで採取している情報の詳細は、/opt/FJSVsnap/READMEに記載されています。

3.6.4 ハードウェア部品交換

ハードウェア部品が故障した場合に、交換する手順を以下に示します。

部品交換の作業を完了した後、“3.4 警告・異常時の対処とリカバリー”のリカバリーを実施してください。

1. 故障箇所の確認

   Appliance Managerの[ホーム]画面のメッセージウィンドウおよび対処ウィンドウの説明や装置の保守ランプから、故障箇所を確認します。故障した箇所の詳細な情報は、ServerView Operations Managerで確認することができます。

   故障箇所を確認したら、富士通サポートセンターに連絡します。

   ポイント

   USBメモリの準備

   スイッチ(ExternalSwitch#1、ExternalSwitch#2)が故障した場合、以降の手順でスイッチの構成定義情報をUSBメモリにコピーする作業がありますので、お持ちのUSBメモリをご準備ください。構成定義情報は約100キロバイトです。USBメモリは、事前にウイルスチェックを実施しておいてください。
   用意したUSBメモリは、コピー後は他の用途で使用せず、適切に保管してください。
   推奨は、富士通コワーコ製のUSBメモリです。

   参考

   ハードウェアの故障を検出した場合、故障した箇所の詳細な情報はServerView Operations Managerで確認してください。

- ServerView Operations Managerを起動するには、Appliance Managerの画面右上の[ServerViewコンソール]リンクをクリックしてください。なお、ServerView Operations Managerを利用するには、管理端末でServerUnit#1、ServerUnit#2の名前解決ができるよう設定されている必要があります(“3.1 管理端末の設定”参照)。
- ServerView Operations Managerについては、“ServerView Suite ServerView Operations Manager V6.21 Server Management 取扱説明書”の“ServerView Operations Managerの使用”を参照してください。
- ServerView Operations Managerでは、ストレージのコントローラーの名称は以下のように表示されます。

ServerViewの表記	装置上の表記
CM00	CM#0
CM01	CM#1

なお、故障箇所が確認できない場合は、SupportDesk契約に基づき富士通サポートセンターに連絡して、故障箇所を特定してください。

2. 交換作業の計画

故障箇所を確認したら、SupportDesk契約に基づき富士通サポートセンターに連絡して、故障したハードウェア部品の交換計画を立てます。
部品交換の作業のために故障した装置を切り離す必要があるか、富士通サポートセンターに確認します。
故障状況によっては、HA Database Readyをシャットダウンして、部品交換作業を行う場合があります。その場合は、富士通サポートセンターの指示に従って行ってください。

3. 故障した装置の切り離し

故障した装置の切り離しを行う場合、Appliance Managerの保守画面にて以下の手順で行います。切り離す装置については、富士通サポートセンターの指示に従ってください。
切り離しにより、サーバの切り替えが発生する場合、データベースサービスが一時的に数秒間停止します。このため、必ず業務が停止中であることを確認して実施してください。

   a. Appliance Managerで[保守]タブを選択し、次に[部品交換準備]タブを開きます。[部品交換準備]画面が開きます。

注意

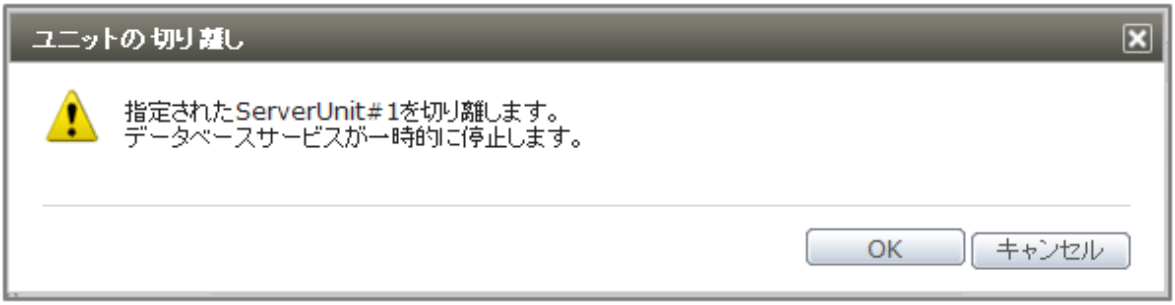
[部品交換準備]画面は、装置の切り離しと、スイッチの構成定義情報のコピーの2つの操作ができます。最初に故障した装置の切り離しの操作を行います。切り離しを行った装置がスイッチの場合だけ、引き続きスイッチの構成定義情報のコピー操作を行います。

b. 富士通サポートセンターからの指示に従って切り離す装置を選択し、[切り離し]ボタンをクリックします。

c. [ユニットの切り離し]のポップアップメッセージが表示されたら、[OK]ボタンをクリックします。故障した装置が切り離されます。

[ユニットの切り離し]のポップアップメッセージ

[ユニットの切り離し]のポップアップメッセージ（サーバの切り替えが発生する場合）



d. 完了のメッセージを確認します。

注意

ServerUnit#1またはServerUnit#2を切り離した場合は、完了のメッセージを確認した後、切り離したServerUnit#1またはServerUnit#2の電源が切断されます。

4. スイッチの構成定義情報のコピー（スイッチ交換時）

スイッチ(ExternalSwitch#1、ExternalSwitch#2)を交換する場合は、スイッチの構成定義情報が必要となります。スイッチの構成定義情報のコピーは、Appliance Managerの保守画面にて以下の手順で行います。本操作は、操作中にUSBメモリの着脱を行うため、装置周辺の管理端末にて実施してください。

a. Appliance Managerで[保守]タブを選択し、次に[部品交換準備]タブを開きます。[部品交換準備]画面が開きます。

b. USBメモリを手元に用意します。

c. [コピー]ボタンをクリックします。

d. [USBメモリのセット]ポップアップメッセージが表示されたら、指示されたサーバのUSBポートにUSBメモリをセットして、[OK]ボタンをクリックします。

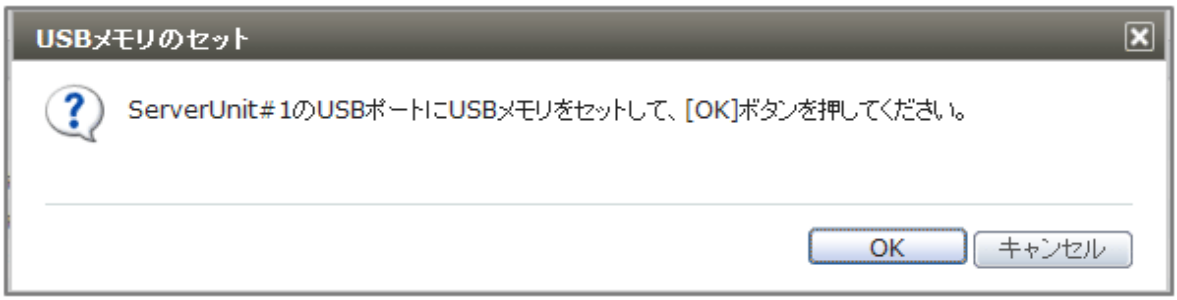


図3.1 ServerUnit#1またはServerUnit#2

注意

用意したUSBメモリが認識されない場合は、別のUSBメモリをご用意ください。推奨は、富士通コワーコ製のUSBメモリです。

e. 完了のメッセージを確認します。

f. USBメモリをサーバから取り外します。
外したUSBメモリは、交換作業の際に弊社保守員に渡してください。

5. 交換作業

弊社保守員がハードウェア部品を交換します。

6. 交換した装置の起動

a. サーバ(ServerUnit#1またはServerUnit#2)の部品を交換して電源が切断されている場合は、交換したサーバの電源ボタンを押して電源を投入します。サーバの電源投入後は、起動が完了するまで約15分待つ必要があります。15分は目安です。

b. データベースを復旧する場合は、“3.4 警告・異常時の対処とリカバリー”の手順2.に戻ってリカバリーを実施します。
データベースを復旧せずにデータベースインターフェースの初期化を行う場合には、“D.2 データベースインターフェースの初期化”を実施します。

注意

交換した装置の起動が完了していない状態でのリカバリーは異常終了(メッセージID：11013)します。その場合は、しばらく待ってから再度実行してください。

3.6.5 容量の追加

運用中にデータ容量が不足した場合には、容量増設オプションを購入することで、使用可能なユーザーデータ量を追加できます。

参照

容量増設オプションの有無による使用可能なユーザーデータ量については、“1.1.3 基本スペック”を参照してください。

運用中に容量を追加する手順を以下に示します。必ず一読してから実施してください。

容量追加作業の計画

容量追加の作業中はデータベースが停止します。そのため容量追加を実施する日時を設定し、その間業務が停止することを事前に広報する必要があります。

容量追加作業の実施

1. 容量追加の作業において、ストレージユニットのIPアドレスが必要となります。“D.3 ネットワークの変更”を参照して、ストレージユニットのIPアドレス（IP1とIP2）を控えておいてください。外部バックアップの運用を行っている場合は、容量追加作業中に外部バックアップが実行されないように、スケジュールを設定してください。
2. Appliance Managerの[ホーム]画面より、HA Database Readyの稼働状態が「正常」になっていることを確認します。
   - 「正常」でない場合には、対処ウィンドウに表示されている対処方法に従って対処してください。ただし、稼働状態が「正常」でない場合でも、11005または11006のメッセージだけが出力されている場合には、対処方法に従う必要はありません。
   - 外部バックアップが実行中の場合には、外部バックアップが完了するまで作業しないでください。
3. Appliance Managerの[電源制御]画面より[シャットダウン]ボタンをクリックし、HA Database Readyをシャットダウンします。
4. 弊社保守員がハードウェアの増設作業を実施します。この際、1.で控えたストレージユニットのIPアドレスを弊社保守員に伝えてください。

5. 弊社保守員がハードウェアの増設および確認作業が完了したことをお客様に通知します。
6. HA Database Readyの電源を投入します。電源投入後は、起動が完了するまで約15分待つ必要があります。15分は目安です。
7. Appliance Managerの[ホーム]画面より、HA Database Readyの稼働状態が「正常」になっていることを確認します。
   - 「正常」でない場合には、対処ウィンドウに表示されている対処方法に従って対処してください。ただし、稼働状態が「正常」でない場合でも、11005または11006のメッセージだけが出力されているときには、対処方法に従う必要はありません。
   - Native SQLインターフェースの場合には、Appliance Managerのメッセージウィンドウを見て、DB管理モード中でないことも確認してください。
8. Appliance Managerの[保守]タブを選択し、次に[容量追加]タブを開きます。[容量追加]画面が開きます。

[容量追加]画面より、[領域再構成]ボタンをクリックします。確認画面が表示されたら、[実行]ボタンをクリックします。
領域再構成では、容量の追加とデータベース資源のバックアップが実行されます。また、領域再構成中は、Appliance Managerの状態が「警告」となります。
領域再構成の所要時間は1時間から7時間です。所要時間は、格納しているデータ量に依存します。
領域再構成が終了すると、Appliance Managerの[ホーム]画面の稼働状態が「正常」となり、メッセージウィンドウに、「領域の再構成を終了しました。」のメッセージが出力されます。
外部バックアップの運用を行っている場合は、外部バックアップが定常実行されるようにスケジュールの設定を戻してください。

ポイント

11005または11006のメッセージだけが出力されている場合

「11005: データ格納先のディスク容量が不足しました。」または「11006: データ格納先の容量が残りわずかです。」の場合、容量追加作業が完了するとこれらのエラー状態が解消されるため、メッセージも消えます。

データベースの運用

Open SQLインターフェース使用時には、「領域の再構成を終了しました。」のメッセージが出力された時点で、データベースのための領域が自動的に拡張されています。

Native SQLインターフェース使用時には、「領域の再構成を終了しました。」のメッセージが出力された後、データベーススペースを作成することで、データベースのための領域を拡張できます。

参照

Native SQLインターフェース使用時の、データベーススペースの作成方法については、“業務開発ガイド(Native SQL編)”の“データベーススペースの作成”を参照してください。

注意

- 領域再構成中に、ハードウェア部品が故障した場合には、“3.6.4 ハードウェア部品交換”を実施してください。「領域再構成が完了していません。領域再構成を再度実行してください。」のメッセージが出力された場合には、再度[領域再構成]ボタンを押してください。
- 容量追加作業前には外部バックアップを取得しておき、領域再構成が終了するまで業務を停止して、常に最新状態にしてから業務を再開することを推奨します。外部バックアップの詳細については、“D.6 外部バックアップ”を参照してください。
  業務再開を急ぐ場合には、“容量追加作業の実施”の手順7.が終了した時点で業務を再開できます。ただし、[領域再構成]ボタンをクリック後、領域再構成が終了するまでの間に両方のサーバが故障した場合、リカバリーボタンによるリカバリーが不可能になりますので注意してください。このような状況であっても、容量追加作業前に外部バックアップを取得しておくことで、サーバ故障の回復後に外部バックアップよりリカバリーを行うことができます。
- “容量追加作業の実施”の手順8.を実行中は、以下の作業は実行できません。
  - バックアップ処理
  - リカバリー処理
  - DB管理モードの設定(Native SQLインターフェースの場合)
  - 修正適用
  - 修正削除
  - ユニットの切り離し
  - データベースインターフェースの初期化
  - 外部バックアップ
  - 外部バックアップを用いたリカバリー

3.6.6 BIOS/ファームウェアの更新

サーバユニット、ストレージユニット、外部接続スイッチのBIOS/ファームウェアを更新するための操作を以下に示します。BIOS/ファームウェアの更新は、二重化された装置のそれぞれに対して実施する必要があります。

サーバユニットおよび外部接続スイッチの場合

1. 更新作業の計画
   定期的に以下のサイトを参照し、最新モジュールをダウンロードします。

   ```
   http://jp.fujitsu.com/platform/server/hadatabase/downloads/
   ```

   BIOS/ファームウェアの更新は、システムを停止して行います。事前に、業務への影響を考慮してBIOS/ファームウェアの更新作業の計画を立てます。
2. システムの停止
   a. BIOS/ファームウェアの更新を行う前に、アプリケーションの停止や、利用者へのアナウンスをします。
   b. HA Database Readyをシャットダウンします。シャットダウンの手順は、“3.7.2 シャットダウン”を参照してください。

3. 更新作業
   ダウンロードした説明ファイルに従って、インストール媒体の作成およびインストールを行います。
   サーバユニットと外部接続スイッチの両方を更新する場合、更新作業の順番は特に決まっていません。なお、装置の更新は各2台のサーバユニットまたは外部接続スイッチに対して実施してください。

4. システムの起動
   BIOS/ファームウェアの更新が終了したら、サーバの電源を投入します。
   電源の投入方法は、“2.1.3 電源の投入”を参照してください。

ストレージユニットの場合

1. ファームウェアの更新情報は、弊社保守員から通知されます。ファームウェアの更新は、システムを停止して行います。事前に、業務への影響を考慮してファームウェアの更新作業の計画を立てます。

2. システムの停止

   a. ファームウェアの更新を行う前に、アプリケーションの停止や、利用者へのアナウンスをします。

   b. HA Database Readyをシャットダウンします。シャットダウンの手順は、“3.7.2 シャットダウン”を参照してください。

3. 更新作業
   弊社保守員が、ストレージユニットのファームウェアを更新します。

4. システムの起動
   ファームウェアの更新が終了したら、サーバの電源を投入します。
   電源の投入方法は、“2.1.3 電源の投入”を参照してください。

3.6.7 保守ランプについて

ハードウェア異常からのリカバリーでは、ハードウェアの異常・警告を示す保守ランプ(エラーランプ)がオレンジ色に点灯・点滅したままになります。このため、保守ランプのエラーを解除する必要があります。

図3.2 ServerUnitの保守ランプ

参考

監視しているServerUnitが再起動したことにより、異常を検知してServerUnitの保守ランプがオレンジ色に点灯・点滅します。

保守ランプのエラーを解除するには、システムを再起動するか、ServerView Operations Managerで以下の操作を行ってください。

1. Appliance Managerの[ホーム]画面のServerViewコンソールをクリックし、ServerView Operations Managerの画面を開きます。

2. ServerView Operations Manager画面からサーバリストでサーバ名をクリックするか、左ペインの[すべてのサーバ]からエントリを選択してコンテキストメニューから「サーバ画面を開く」を選択し、[シングルシステムビュー[サーバ名]]画面を開きます。

3. [シングルシステムビュー[サーバ名]]画面のシステムステータスの[ドライバモニタ]メニューを選択し、[ドライバモニタ]画面を開きます。
4. ステータスをクリアしたい監視コンポーネントを選択して、[承認]ボタンをクリックします。
5. 画面上部の[更新]ボタンをクリックして、ステータスを更新し、ServerView Operations ManagerとAppliance Managerを終了します。
6. 対象サーバの保守ランプの消灯を確認します。

ポイント

操作方法の詳細については、“ServerView Suite ServerView Operations Manager V6.21 Server Management 取扱説明書”の“ドライバモニタ”-“監視コンポーネント”を参照してください。

3.7 データベースシステムの起動と停止

HA Database Readyの電源操作とデータベースシステムの起動/停止は連動しています。HA Database Readyの電源を投入するとデータベースシステムが起動し、シャットダウンを行うとデータベースシステムが停止します。

3.7.1 電源の投入

電源の投入には、以下の2つの方法があります。

- サーバの電源ボタンを押して電源を投入する方法
  “2.1.3 電源の投入”を参照してください。
- 管理端末から、iRMCの電源制御機能を使って電源を投入する方法
  “E.5.1 電源の投入”を参照してください。

電源投入後システムが起動するまで、約15分かかります。15分は目安です。Appliance Managerの[ホーム]画面で稼働状態が正常であることを確認した後、アプリケーションを実行してください。

注意

電源の投入後15分経過してもサーバが起動しない場合は、起動しなかったサーバのiRMC、iRMCに接続されているLANケーブル、またはExternalSwitch#1に異常が発生している可能性があります。
その場合は、起動しなかったサーバの電源ボタンを押して電源を投入してください。

3.7.2 シャットダウン

HA Database Readyのシャットダウンは、以下の手順で行います。

注意

- 必ず、Appliance Managerの画面からシャットダウンするようにしてください。電源ボタンなど他の手段でシャットダウンすると、データベースが正しく停止されません。
- シャットダウン時に、以下の処理が実行中でないかを確認してください。以下を実行中にシャットダウンすると処理はキャンセルされるので、HA Database Readyを再起動後に再度実行してください。
  - アプリケーション
  - バックアップ処理
  - リカバリー処理
  - 外部バックアップ

- 外部バックアップを用いたリカバリー
- 容量追加の領域再構成処理

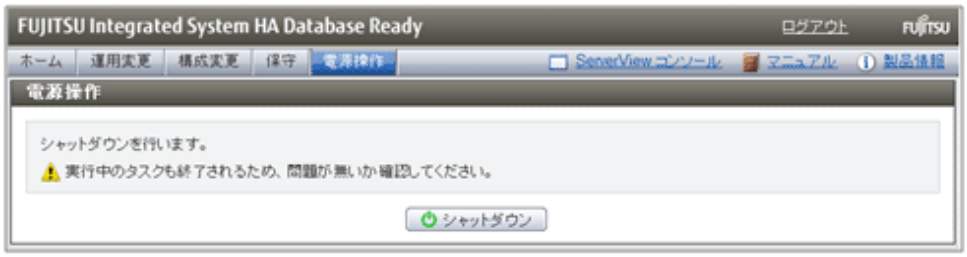
・ シャットダウン時に、以下の処理が実行中でないかを確認してください。以下を実行中にシャットダウンすると処理は中断されるので、弊社保守員に連絡してください。

- 修正適用処理
- 修正削除処理
- ホスト名の変更

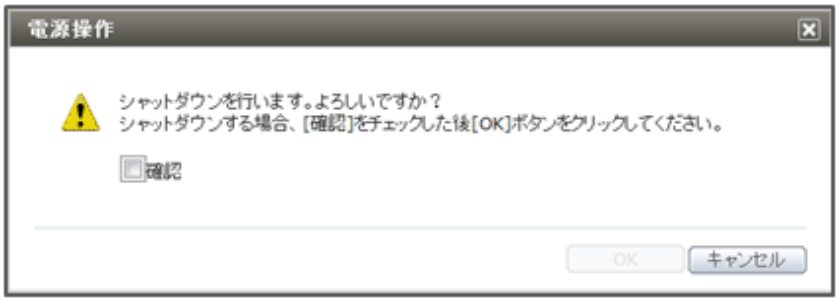
ポイント

シャットダウンを行うと、データベースの運用が停止した後、ServerUnit#1、ServerUnit#2、およびStorageUnitの電源が切断されます。
必要に応じて事前に利用者へのアナウンスなどを行なった上で、シャットダウンを行ってください。

1. Appliance Managerで[電源操作]タブを選択します。[シャットダウン]画面が開きます。



2. [シャットダウン]ボタンをクリックします。
3. 下の画面が表示されますので、[確認]をチェックした後に[OK]ボタンをクリックします。



4. ポップアップメッセージで“シャットダウン要求を発行しました。ブラウザを閉じてください。”と表示されますので、[OK]ボタンをクリックし、Appliance Managerを表示しているWebブラウザを終了します。
[OK]ボタンをクリックして完全にシャットダウンするまで、約15分かかります。15分は目安です。

参考

HA Database Readyが正しくシャットダウンされたかはiRMCの電源制御機能で確認できます。

操作方法については、“E.5.2 電源状態の確認”を参照してください。

付録A　メッセージ一覧

ここでは、HA Database Ready運用中のメッセージの一覧を示します。

参考

メッセージの形式については、“3.3 運用監視”を参照してください。

A.1　FIS-HADBR_AMGRDBで始まるメッセージ

以下にFIS-HADBR_AMGRDBで始まるメッセージの一覧を示します。

"ー"は影響が無いことを示しています。

メッセージID	エラー種別	メッセージ本文	アプリケーションへの影響	データベースの運用への影響
10001	情報	正常に起動しました。	ー	ー
10002	情報	バックアップを開始しました。	ー	ー
10003	情報	バックアップを終了しました。	ー	ー
10004	情報	バックアップ実行中のため、後続のバックアップをキャンセルします。	ー	ー
10005	情報	リカバリーを開始しました。	リカバリーの所用時間、リカバリー中の操作制限については、“表3.2 リカバリー所要時間の目安”を参照してください。	
10006	情報	業務が開始できるようになりました。引き続きリカバリーを継続します。	アプリケーションを開始できます。	ー
10007	情報	リカバリーを終了しました。	ー	ー
10008	情報	リカバリー開始のため、バックアップをキャンセルします。	ー	リカバリー終了後にバックアップを実行してください。
10009	情報	リカバリー実行中にバックアップが要求されました。リカバリーを継続します。		
10010	情報	リカバリー実行中にリカバリーが要求されました。リカバリーを継続します。	ー	ー
10011	情報	保守作業のため、二重化されたデータベースの一方を停止します。	Open SQLインターフェースを選択した場合は、アプリケーションからデータベースへのコネクションが切断される場合があります。コネクションが切断された場合はコネクションを再度接続してください。 Native SQLインターフェースを選択した場合は、実行中のトランザクションがキャンセルされる場合があります。トランザクション	ー

メッセージID	エラー種別	メッセージ本文	アプリケーションへの影響	データベースの運用への影響
			がキャンセルされた場合は、トランザクションを再実行してください。	
10012	情報	DB管理モードを開始しました。	DB管理モード中は、アプリケーションからコネクション接続ができません。	DB管理モード中は、バックアップが実行できません。DB管理モード終了時に自動的にバックアップを実行します。
10013	情報	DB管理モードを終了しました。	－	－
10014	情報	DB管理モードを開始しているため、バックアップをキャンセルします。	－	DB管理モード終了時に自動的にバックアップを実行します。
10015	情報	稼働状態が正常であるため、リカバリーは不要です。	－	－
10016	情報	データベースインターフェースを初期化しました。	－	－
10017	情報	外部バックアップを開始しました。	－	－
10018	情報	外部バックアップを終了しました。	－	－
10019	情報	外部バックアップからのリストアを開始しました。	－	－
10020	情報	領域の再構成を開始しました。	－	－
10021	情報	領域の再構成を終了しました。	－	－
10022	情報	アーカイブログファイル格納先のディスク使用率が閾値（70%）に到達しました。	－	この状態を放置すると11004の警告となりますので、バックアップを実行してください。
10023	情報	データ格納先のディスク使用率が閾値（70%）に到 達しました。	－	Open SQLインターフェースを選択した場合に出力されます。 この状態を放置すると11006の警告となりますので、容量増設オプションを購入するか、不要なデータを削除するなど、データ量を減らしてください。
10024	情報	領域の再構成を開始するため、バックアップをキャンセルします。	－	領域再構成の終了後にバックアップを実行してください。
11001	エラー	二重化したデータベースの一方が停止しました。	Open SQLインターフェースを選択した場合は、アプリケーションからデータベースへのコネクションが切断される場合があります。コネクションが切断された場合はコネクションを再度接続してください。 Native SQLインターフェースを選択した場合は、実行中のトランザクションがキャンセルされる場合があ	データベースの一方が停止しました。切り替えが発生し、業務は継続可能です。性能への影響はありません。 リカバリーを実行して、データベースの二重化状態にしてください。

メッセージID	エラー種別	メッセージ本文	アプリケーションへの影響	データベースの運用への影響
			ります。トランザクションがキャンセルされた場合は、トランザクションを再実行してください。	
11002	エラー	データベースサービスが停止しました。	アプリケーションは実行できません。	運用はできません。リカバリーの実行が必要です。
11003	エラー	アーカイブログファイル格納先のディスク容量が不足しました。	Open SQLインターフェースを選択した場合は、業務への影響はありません。 Native SQLインターフェースを選択した場合は、アプリケーションからのSQL実行がエラーになります。	Open SQLインターフェースを選択した場合は、業務継続が可能です。切り替えは発生しません。性能への影響はありません。リカバリーの実行が必要です。 Native SQLインターフェースを選択した場合は、データベースの運用はできません。リカバリーの実行が必要です。
11004	警告	アーカイブログファイル格納先のディスク容量が残りわずかです。	－	業務継続が可能です。切り替えは発生しません。性能への影響はありません。 アーカイブログファイルの格納先のディスク使用率が90%に到達しています。この状態を放置すると11003のエラーとなりますので、バックアップを実行してください。
11005	エラー	データ格納先のディスク容量が不足しました。	Open SQLインターフェースを選択した場合に出力されます。 アプリケーションからのデータの追加ができなくなります。	データベースの運用ができません。 リカバリーを実行して復旧してください。その後、アプリケーションから不要なデータを削除するなど、データ量を減らしてください。
11006	警告	データ格納先の容量が残りわずかです。	－	Open SQLインターフェースを選択した場合に出力されます。 業務継続が可能です。切り替えは発生しません。性能への影響はありません。 データ格納先のディスク使用率が90%に到達しています。この状態を放置すると11005のエラーとなりますので、容量増設オプションを購入するか、不要なデータを削除するなど、データ量を減らしてください。
11009	エラー	バックアップ先のディスクに異常が発生したため、バックアップが失敗しました。	－	業務継続が可能です。切り替えは発生しません。性能への影響はありません。 この状態を放置するとバックアップが実行できないためデータベースに異常が発生した場合

メッセージID	エラー種別	メッセージ本文	アプリケーションへの影響	データベースの運用への影響
				に復旧できなくなる危険性があります。早急にリカバリーを実行してください。
11011	エラー	アーカイブログファイル格納先のディスクに異常が発生しました。	－	業務継続が可能です。切り替えは発生しません。性能への影響はありません。 この状態を放置するとデータベースに異常が発生した場合に復旧できなくなる危険性があります。早急にリカバリーを実行してください。
11012	エラー	DB管理モードを開始しているため、リカバリーに失敗しました。	Appliance Managerの状態が異常の場合には、アプリケーションは実行できません。	Appliance Managerの状態が警告の場合は業務継続が可能です。異常の場合はデータベースの運用ができません。 DB管理モード終了後にリカバリーしてください。
11013	エラー	リカバリーに失敗しました。	Appliance Managerの状態が異常の場合には、アプリケーションは実行できません。	Appliance Managerの状態が警告の場合は業務継続が可能です。異常の場合はデータベースの運用ができません。 外部バックアップが実行中でない場合は、以下のいずれかの状態でリカバリーを実行したため、リカバリーが完了していません。原因を取り除き、再度リカバリーを実行してください。 ・装置の電源が入っていない ・ハードウェア異常が解決されていない。 また、外部バックアップを用いたリカバリーを実行中の場合には、リカバリー実行後、再度外部バックアップを用いたリカバリーを実行してください。 外部バックアップが実行中の場合は、外部バックアップを中止し、再度リカバリーボタンを押して、リカバリーを実行してください。
11014	警告	バックアップが完了していません。	－	業務継続が可能です。切り替えは発生しません。性能への影響はありません。 バックアップを実行してください。
11015	警告	リカバリーが完了していません。	Appliance Managerの状態が異常の場合には、アプリケーションは実行できません。	Appliance Managerの状態が警告の場合は業務継続が可能です。異常の場合はデータベースの運用ができません。

メッセージID	エラー種別	メッセージ本文	アプリケーションへの影響	データベースの運用への影響
				リカバリーボタンによるリカバリーを実行していた場合には、再度リカバリーボタンを押してリカバリーを実行してください。 外部バックアップを用いたリカバリーを実行していた場合には、再度外部バックアップを用いたリカバリーを実行してください。
11016	エラー	バックアップに失敗しました。	－	業務継続が可能です。切り替えは発生しません。性能への影響はありません。 外部バックアップが実行中の場合は、外部バックアップを中止するか、外部バックアップが完了するまでお待ちください。その後、バックアップを実行してください。 外部バックアップが実行中でない場合は、再度バックアップを実行してください。
11017	エラー	切り替えに失敗しました。	アプリケーションは実行できません。	データベースの運用はできません。 リカバリーを実行してください。
11018	エラー	外部バックアップが実行できません。	－	業務継続が可能です。切り替えは発生しません。性能への影響はありません。 Appliance Managerに他のエラーメッセージが表示されている場合は、対処ウィンドウに表示されている対処方法に従って、対処してください。対処完了後、再度外部バックアップを実行してください。 Appliance Managerに他のエラーメッセージが表示されていない場合は、以下を確認し、対処完了後、再度外部バックアップを実行してください。 ・両方のサーバのバックアップジョブの開始時刻が同一時刻に設定されていることを確認してください ・DB管理モード中の場合は、DB管理モードを終了してください。
11019	エラー	外部バックアップに失敗しました。	－	業務継続が可能です。切り替えは発生しません。性能への影響はありません。

メッセージID	エラー種別	メッセージ本文	アプリケーションへの影響	データベースの運用への影響
				バックアップ製品にエラーメッセージが表示されている場合は、バックアップ製品のドキュメントに従って対処をしてください。対処完了後、再度外部バックアップを実行してください。 Appliance Managerに他のエラーメッセージが表示されている場合は、対処ウィンドウに表示されている対処方法に従って、対処してください。対処完了後、再度外部バックアップを実行してください。
11020	エラー	外部バックアップからのリストアが実行できません。	アプリケーションは実行できません。	データベースの運用はできません。 Appliance Managerに他のエラーメッセージが表示されている場合は、対処ウィンドウに表示されている対処方法に従って、対処してください。対処完了後、再度リストアを実行してください。 Appliance Managerに他のエラーメッセージが表示されていない場合は、以下を確認し、対処完了後、再度外部バックアップからのリカバリーを実行してください。 ・外部バックアップ中の場合は、外部バックアップを中止してください。 ・両方のサーバのリストアジョブの開始時刻が同一時刻に設定されていることを確認してください。
11021	エラー	外部バックアップからのリストアが失敗しました。	アプリケーションは実行できません。	データベースの運用はできません。 バックアップ製品にエラーメッセージが表示されている場合は、バックアップ製品のドキュメントに従って対処をしてください。対処完了後、再度リストアを実行してください。 Appliance Managerに他のエラーメッセージが表示されている場合は、対処ウィンドウに表示されている対処方法に従って、対処してください。対処完了後、再度リストアを実行してください。

メッセージID	エラー種別	メッセージ本文	アプリケーションへの影響	データベースの運用への影響
11022	エラー	領域の再構成が失敗しました。	－	業務継続が可能です。切り替えは発生しません。性能への影響はありません。 Appliance Managerに他のエラーメッセージが表示されている場合は、対処ウィンドウに表示されている対処方法に従って、対処してください。対処完了後、再度[領域再構成]ボタンを押してください。
11023	警告	領域再構成が完了していません。領域再構成を再度実行してください。	－	業務継続が可能です。切り替えは発生しません。性能への影響はありません。 再度、[領域再構成]ボタンを押してください。

A.2 FIS-HADBR_AMGRCMEで始まるメッセージ

以下にFIS-HADBR_AMGRCMEで始まるメッセージの一覧を示します。

“@数字@”は、埋め込み文字列を表します。実際に出力されるメッセージでは、文字列が出力されます。

"－"は影響がないことを示しています。

メッセージID	エラー種別	メッセージ本文	アプリケーションへの影響	データベース運用への影響
10001	エラー	メールの送信に失敗しました。SMTPサーバの状態を確認し対処してください。エラー詳細: [*詳細メッセージ*]	－	業務への影響はありません。SMTPサーバの状態を確認してください。
10002	エラー	正常稼働通知に失敗しました。	－	業務への影響はありません。SMTPサーバの状態を確認してください。
10003	エラー	@1@の@2@からの応答がありません。	－	監視対象@1@の@2@のネットワーク接続を確認してください。ネットワーク接続に不具合がある場合、この状態を放置すると監視対象@1@の異常が検知できないため問題が拡大する可能性があります。なお、何らかの理由で監視対象の電源が投入されていない場合にも本メッセージが出力されます。
10004	警告	[*ホスト名*]のAppliance Managerが異常停止しました。	－	業務継続が可能です。この状態でもう一方のAppliance Managerが停止した場合、データベースの運用ができなくなる場合があります。“J.2 問合せ時に必要な情報”を参照し、早急

メッセージ ID	エラー種別	メッセージ本文	アプリケーションへの影響	データベース運用への影響
				に弊社保守員へ連絡してください。
10005	エラー	両方のAppliance Managerが異常停止しました。	アプリケーションの実行が不可能である場合があります。	業務継続が不可能である場合があります。“J.2 問合せ時に必要な情報”を参照し、早急に弊社保守員へ連絡してください。

付録B　端末の条件

HA Database Readyで用意していただく以下の端末について説明します。

- セットアップ用PC(HA Database Readyのセットアップ時にだけ使用)
- 管理端末

B.1　端末の条件

セットアップ用PCと管理端末には、以下の条件を満たす端末を準備してください。

- OSがWindowsであること (注1)
- 画面解像度が1024×768以上であること
- Internet Explorer 9.0、10.0または11.0のバージョンがインストールされていること
- 端末エミュレータソフトウェア(SSH2対応)がインストールされていること(注2)

注1) OS

以下のいずれかが必要です。

- Windows Vista(R) Ultimate
- Windows Vista(R) Enterprise
- Windows(R) 7 Ultimate
- Windows(R) 7 Enterprise
- Windows(R) 7 Professional
- Windows(R) 8 Pro
- Windows(R) 8 Enterprise
- Windows(R) 8.1 Pro
- Windows(R) 8.1 Enterprise
- Microsoft(R) Windows Server(R) 2008 Standard
- Microsoft(R) Windows Server(R) 2008 Enterprise
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V
- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V
- Microsoft(R) Windows Server(R) 2008 Standard
- Microsoft(R) Windows Server(R) 2008 Enterprise
- Microsoft(R) Windows Server(R) 2008 Standard without Hyper-V
- Microsoft(R) Windows Server(R) 2008 Enterprise without Hyper-V
- Microsoft(R) Windows Server(R) 2008 R2, Standard
- Microsoft(R) Windows Server(R) 2008 R2, Enterprise
- Microsoft(R) Windows(R) Small Business Server 2011 Essentials

ー Microsoft(R) Windows Server(R) 2012 Datacenter

ー Microsoft(R) Windows Server(R) 2012 Standard

ー Microsoft(R) Windows Server(R) 2012 Essentials

ー Microsoft(R) Windows Server(R) 2012 Foundation

注2) 端末エミュレータソフトウェア

セットアップ用PCには必須ですが、管理端末ではサーバユニットへのログインする場合にだけ必要です。

B.2 Webブラウザの設定

Webブラウザ上でAppliance Managerを正しく表示するためのWebブラウザの設定について説明します。

Appliance Managerは以下の設定で画面が設計されています。Webブラウザ上で表示が正しくない場合は、以下のように設定してください。

・ ブラウザの文字サイズ、画面サイズを標準の大きさで使用してください。標準の大きさにするには以下の手順のいずれかを実施してください。

ー メニューから「表示」→「拡大」→「100%」を選択する。

ー メニューから「表示」→「文字のサイズ」→「中」を選択する。

・ ブラウザの「Webページ フォント」に「MS Pゴシック」を設定してください。

1. メニューから「ツール」→「インターネットオプション」を選択する。
2. 「全般」タブの「フォント」ボタンをクリックし、「Webページフォント」に「MS Pゴシック」を設定する。

・ ブラウザでタブ ブラウズ機能を有効にしている場合は、新しいウィンドウでポップアップを開くように設定してください。

1. メニューから「ツール」→「インターネットオプション」を選択する。
2. 「全般」タブの「タブ」の「設定」ボタンをクリックし、「ポップアップの発生時」の「常に新しいウィンドウでポップアップを開く」を選択する。

・ ブラウザでアニメーションを再生できるように設定してください。

1. メニューから「ツール」→「インターネットオプション」を選択する。
2. 「詳細設定」タブから、「マルチメディア」の「Webページのアニメーションを再生する」を有効にする。

Internet Explorerを使用する場合

以下は、Internet Explorer 9.0の設定例です。

1. メニューから「ツール」→「インターネットオプション」を選択する。
2. 「セキュリティ」タブを選択し、「セキュリティ設定を表示または変更するゾーンを選択してください。」から、「信頼済みサイト」を選択する。
3. 「サイト」ボタンをクリックし、信頼済みサイトに「https://*管理用のIPアドレス*」を登録する。
4. 「このゾーンのセキュリティレベル」で、[レベルのカスタマイズ]ボタンをクリックし、[セキュリティ設定]ダイアログで[ダウンロード]の[ファイルのダウンロード]を有効にする。
5. 管理端末には以下も設定する。

a. 「セキュリティ」タブの「保護モードを有効にする」をチェックし、「レベルのカスタマイズ」を選択する。

b.「ActiveXコントロールとプラグイン」→「ActiveXコントロールとプラグインの実行」で、「ダイアログを表示する」または「有効にする」を選択して「OK」をクリックする。

Windows Server 2008、またはWindows Server 2012を使用する場合

以下のうち、いずれかの設定をしてください。

a. about:blankおよびabout:internetを信頼済みサイトに登録する。

b. 以下の設定をする。以下は、Windows Server 2008の例です。

1.「スタート」メニュー→「管理ツール」を選択します。

2.「サーバーマネージャー」から、「セキュリティ情報」の「IE ESCの構成」を選択して、「Internet Explorerセキュリティ強化の構成」を起動します。

3.「Administratorグループ(A):」と「Usersグループ(U):」の設定を両方とも「オフ」を設定してください。

付録C　使用可能な文字コード一覧

データベースに使用可能な文字コードの一覧を以下に示します。

データベースインターフェース	文字コード
Open SQL	EUC_CN EUC_JP EUC_JIS_2004 EUC_KR EUC_TW ISO_8859_5 ISO_8859_6 ISO_8859_7 ISO_8859_8 KOI8R KOI8U LATIN1 LATIN2 LATIN3 LATIN4 LATIN5 LATIN6 LATIN7 LATIN8 LATIN9 LATIN10 MULE_INTERNAL SQL_ASCII UTF8 WIN866 WIN874 WIN1250 WIN1251 WIN1252 WIN1253 WIN1254 WIN1255 WIN1256 WIN1257 WIN1258
Native SQL	EUC_S90 SJIS UTF8

付録D　運用の詳細設定

運用の詳細設定について説明します。

セットアップ完了後に、お客様のやりたいことに合わせて、設定の確認や変更ができます。

やりたいこと	参照先
HA Database Readyのデータベースインターフェースやipアドレスを確認したい	“D.1 データベースインターフェースとIPアドレスの確認”
セットアップ時に選択したデータベースインターフェースを変更したい	“D.2 データベースインターフェースの初期化”
設置場所の変更等で、ネットワーク設定を変更したい	“D.3 ネットワークの変更”
管理ネットワーク内に、ルータなどのゲートウェイを設定し、異なるサブネットのネットワークを接続したい	“D.4 管理ネットワークの経路設定”
開発フェーズから本運用に移行するなどAppliance Managerの[ホーム]画面のメッセージウィンドウに表示されているメッセージを消去したい	“D.5 メッセージの消去”
災害発生時に備えて、ストレージに自動退避しているデータベース資源を、外部のバックアップ環境にも退避したい	“D.6 外部バックアップ”
HA Database Readyのホスト名を変更したい	“D.7 ホスト名の変更”
データベースの格納データを暗号化したい	“D.8 格納データの暗号化”

D.1　データベースインターフェースとIPアドレスの確認

HA Database Readyで使用しているデータベースインターフェースとIPアドレスは、以下の手順で確認してください。

1. ServerUnit#1に、スーパーユーザーでログインします。ログイン方法については、“付録G サーバへのログイン方法”を参照してください。
2. 以下のコマンドを実行します。HA Database Readyで使用しているIPアドレスが表示されます。

```
# /opt/FJSVaplamdb/bin/show_setup.sh
```

出力例

```
FUJITSU Integrated System HA Database Ready Setup List
Interface          : Open SQL Interface , UTF8
Port Number        : 26500
IPv4
  Application LAN  : 172.20.10.10 , 172.20.10.11
         Gateway   : 172.20.10.1
         Netmask   : 255.255.255.0
  Management LAN
      Server Unit  : 192.168.1.10 , 192.168.1.11
         iRMC      : 192.168.1.20 , 192.168.1.21
      Storage Unit : 192.168.1.220 , 192.168.1.230
   External Switch : 192.168.1.100 , 192.168.1.101
         Netmask   : 255.255.255.0
  Interconnect LAN : 192.168.2.* , 192.168.3.* , 192.168.4.*
IPv6
  Application LAN  : - , -
           Gateway : -
       Prefix Size : -
```

未指定の項目は、"-"と表示されます。

D.2　データベースインターフェースの初期化

セットアップの誤りの修正や、データベースの設計変更のため、HA Database Readyのデータベースインターフェースの設定を初期化して、インターフェースを再設定する場合は、以下の手順で実施してください。

1. 初期化を実行する前に、アプリケーションの停止や、利用者へのアナウンスをします。
2. ServerUnit#1に、スーパーユーザーでログインします。ログイン方法については、“付録G サーバへのログイン方法”を参照してください。
3. 以下に示すコマンドを実行し、データベースインターフェースを初期化します。

```
# /opt/FJSVaplamdb/bin/DBif_Initialize.sh
```

4. コマンドを実行すると、以下の項目の入力を求められます。
すべての項目の入力後に、データベースの初期化処理が実行されます。
   a. 初期化処理の実行確認
   b. データベースインターフェース
   c. データベースの文字コード
   d. ポート番号

注意

ポート番号に指定可能な値は、5432および26500～26999です。初期値は以下です。

- Open SQLインターフェースの場合　：26500
- Native SQLインターフェースの場合：26551

以下に、コマンドの実行例を示します。**太字**は、お客様が入力する項目です。

```
# /opt/FJSVaplamdb/bin/DBif_Initialize.sh
********************** WARNING ***************************
This script will initialize database preferences.
Initialization includes DELETING ALL DATA IN YOUR DATABASE.

Type "OK" to continue, or cancel initialization.
> OK                                              …a. 初期化処理の実行確認

Select database type. (0:Native SQL interface, 1:Open SQL interface)
(0:Native/[1:Open]): 1                            …b. データベースインターフェース

Open SQL interface is selected.

Select database character set.
UTF8 is default and recommended character set.
Do you want to change DB character set?
(y/[n](use UTF8)): n                              …c. データベースの文字コード

UTF8 is selected for DB character set.

Input port number for database service.
Port number must be 5432 or 26500-26999(inclusive).
[default: 26500]: 26500                            …d. ポート番号

[ Initialization information ]
Database type    : Open SQL interface
Character set    : UTF8
Port number      : 26500
```

```
Type "OK" to proceed.
Once proceeded, all data will be deleted and there's NO UNDO.
Type "exit" to cancel initialization.
(OK/exit): OK

************************************
Initialization completed.
You can use new database service now.
(Administrator ID was not changed. You can use old one.)
FIS-HADBR_AMGRDB: INFO: 10016: データベースインターフェースを初期化しました。
```

5. 初期化の所要時間の目安は、15分から1時間です。時間はデータベースの容量に依存します。また、初期化中は画面に何も表示されません。初期化が完了したら、"Initialization completed." 以降の文字列が表示されます。その後、Appliance Managerにログインし、[ホーム]画面で、稼働状態が正常であることを確認します。

注意

- データベースインターフェースを初期化すると、データベースの定義やデータベースに格納されていたデータなど、すべての設定が破棄されます。
- データベースインターフェースの初期化中は、HA Database Readyのすべての機能を使用できません。
- データベースインターフェースの初期化は、ハードウェアに異常が発生している場合には、実施できません。ハードウェアに異常が発生している場合には、"3.6.4 ハードウェア部品交換" の手順を実施してください。

D.3 ネットワークの変更

HA Database Readyの設置場所を変更する場合など、HA Database Readyで使用している業務ネットワーク、内部ネットワーク、または管理ネットワークのIPアドレスを変更する場合は、以下の手順で実施してください。

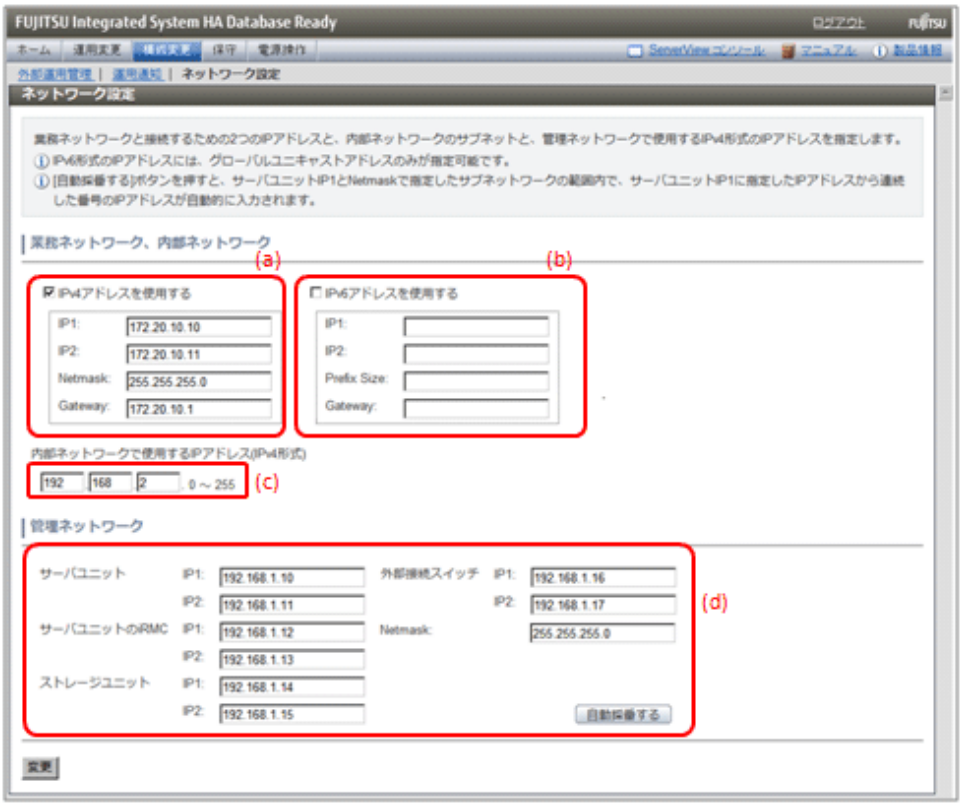
注意

- IPアドレスの変更には、変更前の管理用のIPアドレスが必要です。
- 変更するIPアドレスが、接続されている機器で使用されていないことを確認してください。

1. IPアドレスの変更時はデータベースの運用が停止するので、事前にアプリケーションの停止や、利用者への停止アナウンスをします。
2. 管理端末で、Appliance Managerにログインします。
   Webブラウザのアドレスバーに、以下のURLを入力します。

```
https://管理用のIPアドレス/appmgr/
```

3. Appliance Managerの[ホーム]画面から、[構成変更]タブを選択し、次に[ネットワーク設定]タブを開きます。
[ネットワーク設定]画面には、初期値として現在の設定値が表示されます。



4. 変更するIPアドレスを指定します。

   a. 業務ネットワークのIPアドレス(IPv4)を変更する場合
   [IPv4アドレスを使用する]をチェックし、業務ネットワークと接続するための2つのIPv4形式のIPアドレスを指定します。

   b. 業務ネットワークのIPアドレス(IPv6)を変更する場合
   [IPv6アドレスを使用する]をチェックし、業務ネットワークと接続するための2つのIPv6形式のIPアドレスを指定します。

   c. 内部ネットワークのIPアドレスを変更する場合
   [内部ネットワークで使用するIPアドレス(IPv4形式)]に、内部ネットワークで使用するIPv4形式のIPアドレスを指定します。

   d. 管理ネットワークのIPアドレスを変更する場合
   管理ネットワークで使用するIPv4形式のIPアドレスを指定します。
   管理ネットワークの各入力欄に、管理ネットワークで使用するIPv4形式のIPアドレスを指定します。

5. [変更]ボタンをクリックします。
   ネットワークの設定が変更され、ServerUnit#1およびServerUnit#2がシャットダウンします。

6. 管理ネットワークのサーバユニットのIPアドレスを変更した場合は、続いて故障監視のための設定を行います。管理ネットワークのサーバユニットのIPアドレスの変更がなければ、手順12.に進んでください。
   ServerUnit#1およびServerUnit#2をシャットダウンしたままで、故障監視のための設定を行います。
   Webブラウザに、サーバユニットのiRMCの変更後のIP1のアドレスを指定してください。

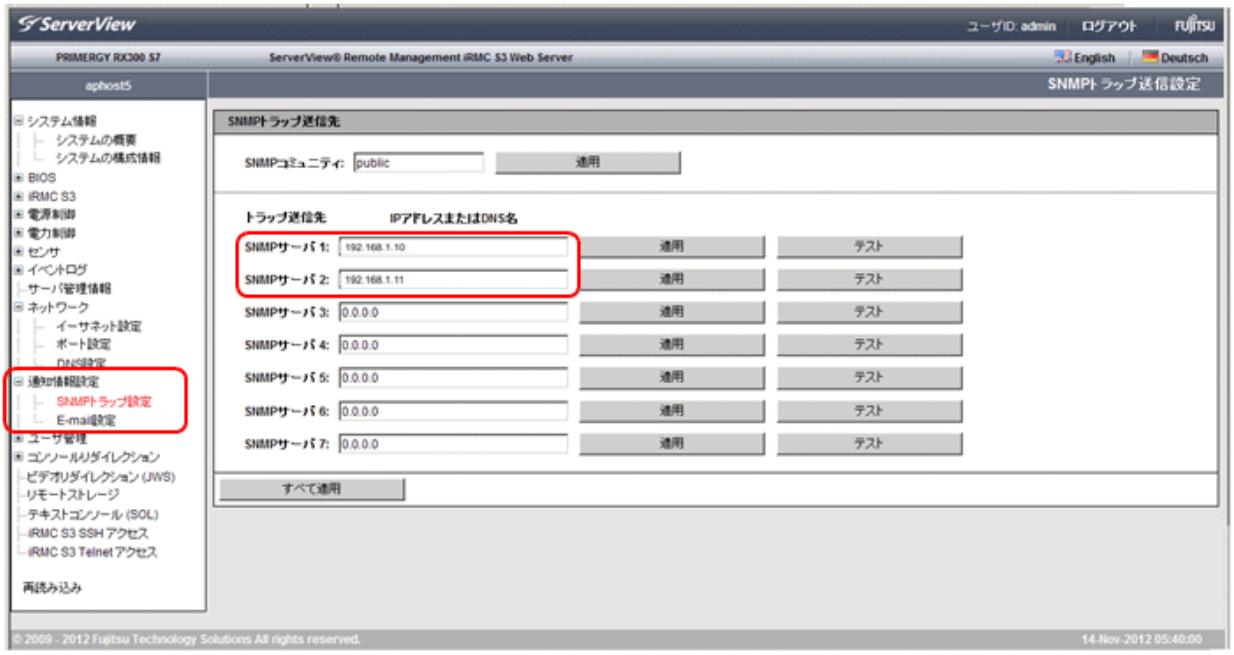
   ```
   http://サーバユニットのiRMCの変更後のIP1のアドレス/
   ```

   認証画面が表示されます。ユーザー名：「admin」、パスワードはセットアップ時に変更したパスワードでアクセスしてください。

注意

認証画面が表示されない場合には、しばらく待ってから、再度、Webブラウザにサーバユニットの iRMCのIP1のアドレスを指定してアクセスしてください。

7. 認証が完了するとServerViewの画面が表示されます。
   画面が英語で表示されている場合、画面右上の[日本語]リンクをクリックしてください。
8. 左画面のナビゲーションエリアのメニューで[通知情報設定]の[SNMPトラップ設定]を選択すると、以下の画面が表示されます。



9. 右画面の[SNMPトラップ送信先]の[SNMPサーバ1]の[IPアドレスまたはDNS名]欄に、変更後の管理ネットワークのサーバユニットのIP1を設定します。次に、[SNMPサーバ2]の[IPアドレスまたはDNS名]欄に、変更後の管理ネットワークのサーバユニットのIP2を設定し、[すべて適用]ボタンをクリックしてください。
10. Webブラウザに、サーバユニットのiRMCの変更後のIP2のアドレスを指定してください。

    ```
    http://サーバユニットのiRMCの変更後のIP2のアドレス/
    ```

    認証画面が表示されます。ユーザ名：「admin」、パスワードはセットアップ時に変更したパスワードでアクセスしてください。
11. 手順7.～9.を実行してください。
12. HA Database Readyの電源を投入し、Appliance Managerの[ホーム]画面に表示される稼働状態の表示でHA Database Readyの起動を確認したら、アプリケーションを再開し、利用者へ再開をアナウンスします。電源の投入については、“3.7.1 電源の投入”を参照してください。

ポイント

- HA Database Readyを移設する場合は、上記の手順12の前に機器の移設を実施してください。
  その際、StorageUnitの電源を切断してください。電源を切断するには、“設置ガイド”の“StorageUnitの装置図(DX80 S2)”を参照して電源ボタンの位置を確認し、長押しします。

・ 機器にすでに設定されたIPアドレスを、別の機器のIPアドレスとして再設定する場合は、双方の機器を一旦、未使用のIPアドレスに設定して、ネットワークの変更を完了させてください。その後、変更したいIPアドレスを設定して、再度ネットワークの変更を実施してください。

D.4　管理ネットワークの経路設定

管理ネットワーク内に、ルータなどのゲートウェイを設定し、異なるサブネットのネットワークを接続する場合は、以下の手順で経路を設定してください。

1. 管理ネットワークの経路を変更する前に、アプリケーションの停止や、利用者へのアナウンスをします。
2. ServerUnit#1に、スーパーユーザーでログインします。ログイン方法については、“付録G サーバへのログイン方法”を参照してください。
3. 以下のコマンドを使って、管理ネットワークの経路を設定します。
   a. 管理ネットワーク経路を追加する場合

   ```
   # /opt/FJSVaplamdb/bin/add_mng_route.sh ネットワークアドレス -m サブネットマスク -gw ゲートウェイアドレス
   ```

   例
   以下のネットワーク環境の場合(“図D.1 セットアップ後のネットワークの接続例”を参照してください)

   - お客様の管理用のネットワークアドレスが172.30.10.0/24
   - 管理ネットワークのゲートウェイ(ルータなど)のHA Database Ready側のIPアドレスが192.168.1.1

   ```
   # /opt/FJSVaplamdb/bin/add_mng_route.sh 172.30.10.0 -m 255.255.255.0 -gw 192.168.1.1
   ```

   b. 管理ネットワーク経路を削除する場合

   ```
   # /opt/FJSVaplamdb/bin/del_mng_route.sh ネットワークアドレス -m サブネットマスク
   ```

   c. 管理ネットワーク全経路を削除する場合

   ```
   # /opt/FJSVaplamdb/bin/del_mng_all_route.sh
   ```

   d. 追加した管理ネットワーク経路を表示する場合

   ```
   # /opt/FJSVaplamdb/bin/dsp_mng_all_route.sh
   ```

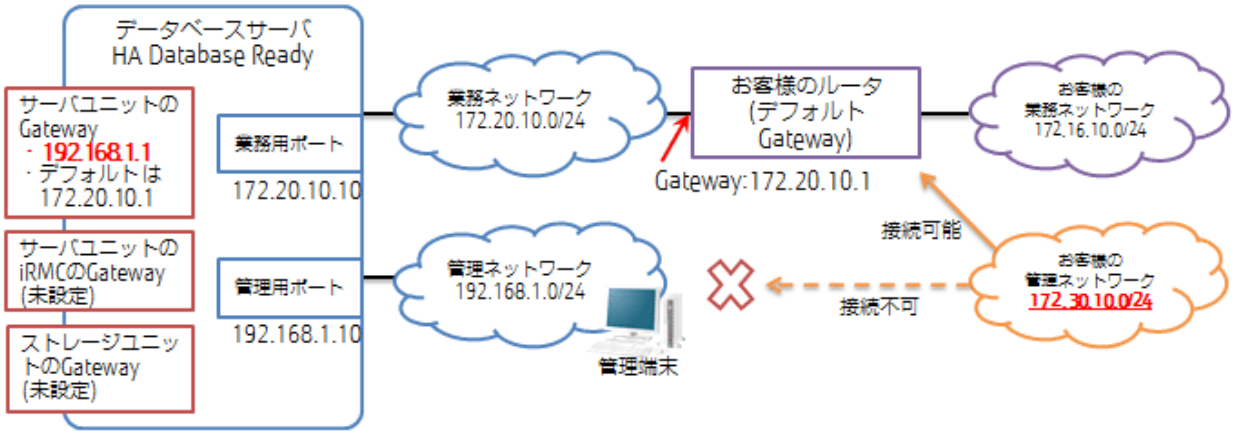
4. ServerUnit#1からログアウトします。
5. ServerUnit#2に、スーパーユーザーでログインし、手順3.を実施した後、ログアウトします。
6. HA Database Readyをシャットダウンします。
   シャットダウンについては、“3.7.2 シャットダウン”を参照してください。
7. HA Database Readyの電源を投入してください。
   電源の投入については、“3.7.1 電源の投入”を参照してください。
8. Appliance Managerの[ホーム]画面に表示される稼働状態の表示でHA Database Readyの起動を確認したら、アプリケーションを再開し、利用者へ再開をアナウンスします。

注意

・ 外部ネットワークからゲートウェイを経由してHA Database Readyに接続する場合は、業務ネットワークまたは管理ネットワークのどちらか一方しか接続できません。
HA Database Readyのセットアップ後は、業務ネットワークのデフォルトゲートウェイを経由して業務ネットワークにだけ接続できます。外部ネットワークの管理端末や運用管理サーバを管理ネットワークに接続するためには、管理ネットワークの経路設定を行ってください。
ただし、管理ネットワークの経路設定をすることで、管理端末や運用管理サーバは、業務ネットワークに接続できなく

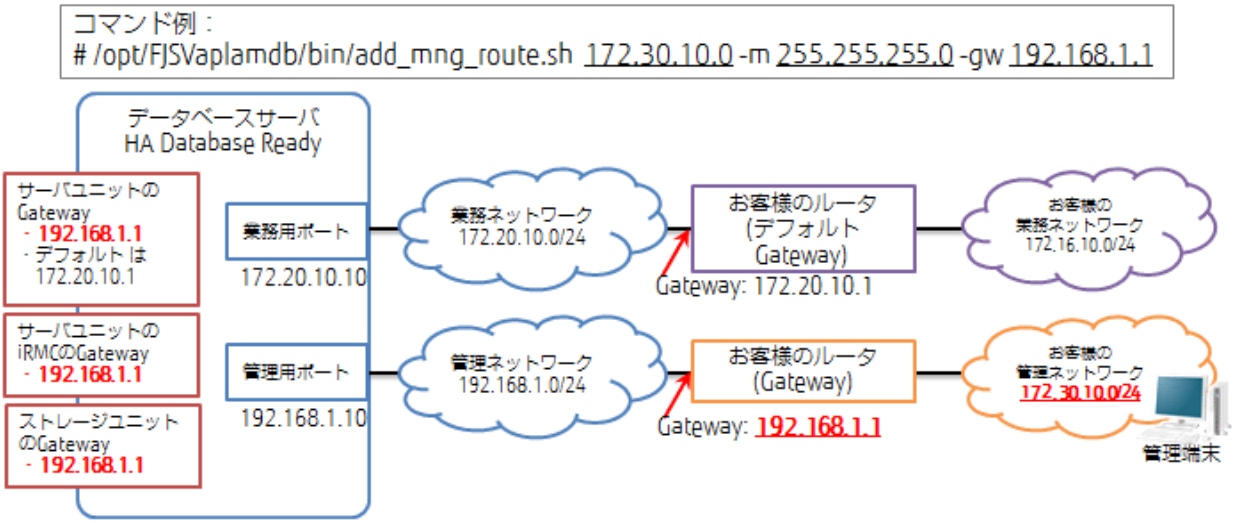
なります。
なお、お客様のネットワークのサブネットが、業務と管理に分かれていない場合は、ネットワーク管理者に相談してください。

図D.1 セットアップ後のネットワークの接続例



・ 管理ネットワーク経路の追加を実行すると、指定されたゲートウェイアドレスは、サーバユニットだけでなく、サーバユニットのiRMCおよびストレージユニットのゲートウェイにも設定されます。なお、サーバユニットのiRMCおよびストレージユニットに設定できるゲートウェイは1つなので、複数の経路を設定した場合には、最後に指定されたゲートウェイアドレスがサーバユニットのiRMCおよびストレージユニットに設定されます。

図D.2 管理ネットワークの経路設定を行った場合の接続例



・ サーバユニットのiRMCとストレージユニットには、異なるゲートウェイを設定できません。

・ サーバユニットのiRMCおよびストレージユニットのゲートウェイを変更する場合には、管理ネットワーク経路の削除や管理ネットワーク全経路の削除を実施しても、サーバユニットのiRMCおよびストレージユニットのゲートウェイは削除されません。新しく管理ネットワークの経路を追加することで、変更を実施してください。

D.5　メッセージの消去

HA Database Readyをテスト運用から本運用に移行する場合などに、Appliance Managerの[ホーム]画面のメッセージウィンドウに表示されているメッセージを消去するには、以下の手順で実施してください。

注意

- 通常の運用の途中では、メッセージウィンドウの表示の消去は行わないでください。
- 本作業は、Appliance Managerの[ホーム]画面の稼働状態が「正常」になっていることを確認してから実施してください。

1. Appliance Managerが一時的に停止するため、必要に応じて利用者へアナウンスします。
2. いずれかのサーバユニットに、スーパーユーザーでログインします。ログイン方法については、“付録G サーバへのログイン方法”を参照してください。
3. 以下に示すコマンドを実行し、メッセージを消去します。

```
# /opt/FJSVaplam/bin/clearMessage.sh
```

4. Appliance Managerの[ホーム]画面の表示を確認し、利用者へ再開をアナウンスします。

注意

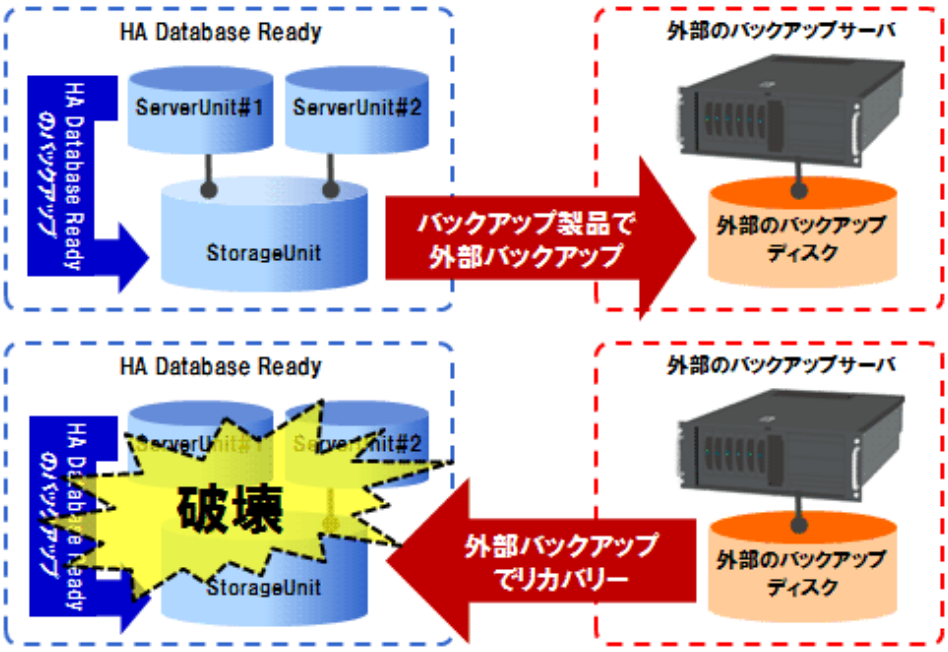
手順3.で“Error occurred.”のメッセージが表示された場合は、内部エラーが発生している可能性があります。“J.2 問合せ時に必要な情報”を参照し、弊社保守員へ連絡してください。

D.6 外部バックアップ

HA Database Readyでは、NetVault Backupなどのバックアップ製品と連携することで、外部バックアップが実行できます。外部バックアップでは、“3.5.2 バックアップ”によりストレージ上に取得したバックアップを、バックアップ製品を用いて、お客様が用意した外部のバックアップサーバに退避します。

外部バックアップを利用することで、被災時にHA Database Readyのサーバとストレージがすべて破壊されてしまった場合や、誤ったSQLを実行してしまった場合に、前回HA Database Readyのバックアップが完了した時点までデータベースを復旧できます。

図D.3 外部バックアップの運用例



ポイント

外部バックアップを利用するには、以下の機能を持つバックアップ製品が必要です。

- バックアップジョブ/リストアジョブ機能
- バックアップ実行前とバックアップ実行後に実行するコマンドを登録する機能
- リストア実行前とリストア実行後に実行するコマンドを登録する機能

D.6.1 外部バックアップの事前準備

バックアップ製品と連携して外部バックアップを実行するためには、以下の準備が必要です。以下の準備を1度実施することで、外部バックアップが定期的に実行されます。

1. **外部のバックアップサーバと外部のバックアップ媒体を準備します。**
   外部バックアップのためには、外部のバックアップサーバを用意し、HA Database Readyのネットワークに接続します。外部のバックアップ媒体は、外部のバックアップサーバにマウントします。以下に、製品ごとの1世代あたりに必要な最大の容量を示します。

データベースインターフェース	1世代あたりに必要な最大容量			
	2CPUモデル	2CPUモデル+容量増設追加オプション	4CPUモデル	4CPUモデル+容量増設オプション
Open SQL	3.0TB	5.0TB	6.0TB	8.0TB
Native SQL	5.9TB	10.0TB	12.0TB	14.1TB

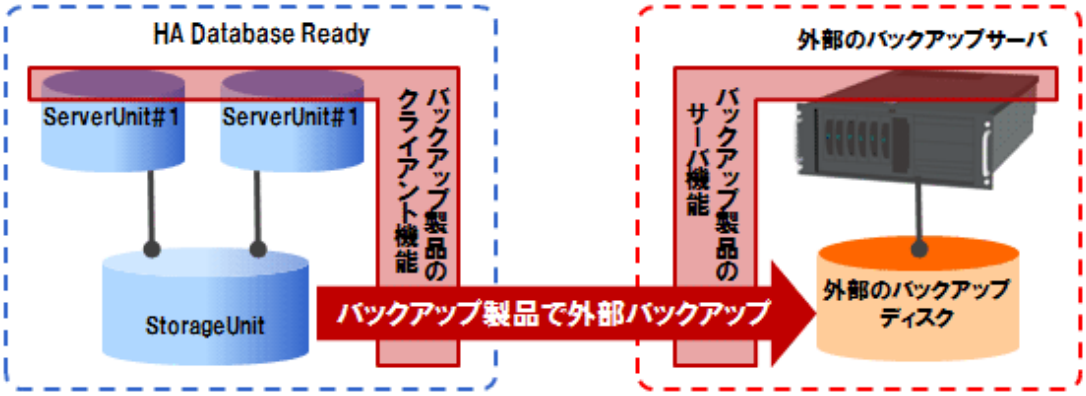
ポイント

外部バックアップの所要時間を短縮するために、以下の構成を推奨します。

ー ネットワークは10GbEで構成する。

ー 外部のバックアップ媒体はRAID 1+0構成にするなど、高速な媒体を使用する。

2. **バックアップ製品をインストールします。**
外部のバックアップサーバにバックアップ製品のサーバ機能をインストールします。
HA Database ReadyのServerUnit#1とServerUnit#2に、それぞれ別々にスーパーユーザーでログインします。ログイン方法については、“付録G サーバへのログイン方法”を参照してください。ServerUnit#1とServerUnit#2にバックアップ製品のクライアント機能を転送してインストールします。インストール先は、/opt配下に作成したディレクトリを指定してください。バックアップ製品のインストール方法は、バックアップ製品のドキュメントに従ってください。
HA Database Readyにインストールするバックアップ製品で使用可能なポートは、5432および26500～26999です。これらのポートは購入時には開放されていないため、バックアップ製品の機能もしくはOSの機能を用いて、必要なポートを開放してください。



3. **バックアップ製品にバックアップジョブを登録します。**
バックアップ製品には、バックアップジョブという機能があり、一度設定を行うことで定期的に外部バックアップを実行することが可能です。バックアップジョブは、ServerUnit#1とServerUnit#2のそれぞれに登録します。
バックアップジョブには、以下の項目について設定します。

   a. バックアップジョブのスケジュールを登録
   バックアップジョブでは、実行する周期や開始時刻を設定してください。実行する周期は、お客様の運用に合わせて設定してください。

   ### ポイント

   - バックアップジョブの開始時刻は、ServerUnit#1のバックアップジョブとServerUnit#2のバックアップジョブの両方とも、HA Database Readyのバックアップの開始時刻の5分後に設定してください。
   - 外部バックアップは、HA Database Readyのバックアップが終了した時点で自動的に開始されます。

   b. 外部バックアップのディレクトリを登録
   それぞれのバックアップジョブがバックアップするディレクトリとして、以下を登録します。

表D.1 バックアップジョブの一覧

データベースインターフェース	バックアップジョブ	バックアップ元	バックアップ先(外部のバックアップ媒体上)	1世代あたりの容量			
				2CPUモデル	2CPUモデル+容量増設オプション	4CPUモデル	4CPUモデル+容量増設オプション
Open SQL	ServerUnit #1のジョブ	ServerUnit#1上の以下2つ。 ・/disk1/pg/archived_xlog/ ・/disk2/pg/	共通のバックアップ先	3.0TB	5.0TB	6.0TB	8.0TB
	ServerUnit #2のジョブ	ServerUnit#2上の以下2つ。 ・/disk1/pg/archived_xlog/ ・/disk2/pg/					
Native SQL	ServerUnit #1のジョブ	ServerUnit#1上の以下2つ。 ・/disk2/rdb/backup/ ・/disk4/rdb/cntl_back/	ServerUnit #1用のバックアップ先	2.95TB	5.0TB	6.0TB	7.05TB
	ServerUnit #2のジョブ	ServerUnit#2上の以下2つ。 ・/disk2/rdb/backup/ ・/disk4/rdb/cntl_back/	ServerUnit #2用のバックアップ先	2.95TB	5.0TB	6.0TB	7.05TB

c. バックアップ実行前とバックアップ実行後に実行するコマンドを登録
バックアップジョブには、バックアップ実行前に実行するコマンドと、バックアップ実行後に実行するコマンドを登録できる機能があります。以下のコマンドをバックアップ製品からアクセスできるディレクトリにコピーし、バックアップジョブに登録します。

状況	コマンド名
バックアップ実行前に実行するコマンド	/opt/FJSVaplamdb/bin/apl_prebackup_from_StorageUnit.sh
バックアップ実行後に実行するコマンド(注)	/opt/FJSVaplamdb/bin/apl_postbackup_from_StorageUnit.sh

注) バックアップ製品ごとにカスタマイズすることを推奨します。

例

バックアップ製品でエラーが発生した際にAppliance Managerにメッセージを表示する場合

「バックアップ実行後に実行するコマンド」をカスタマイズすることで、外部バックアップ中にバックアップ製品でエラーが発生した場合に、Appliance Managerのメッセージウィンドウに「外部バックアップに失敗しました。」のメッセージを出力させることができます。
この場合、以下のようなコマンドを作成し、バックアップ製品からアクセスできるディレクトリに置いて実行権を付けた後、バックアップジョブに登録します。

バックアップ実行後に実行するコマンドの例(NetVault Backup使用時)を以下に示します。

```
#!/bin/bash

if [ "${NV_STATUS}" = "FAILED" ] ; then
      /opt/FJSVaplamdb/bin/apl_postbackup_from_StorageUnit.sh 1   …(1)
      exit $?
else
      /opt/FJSVaplamdb/bin/apl_postbackup_from_StorageUnit.sh 0   …(2)
```

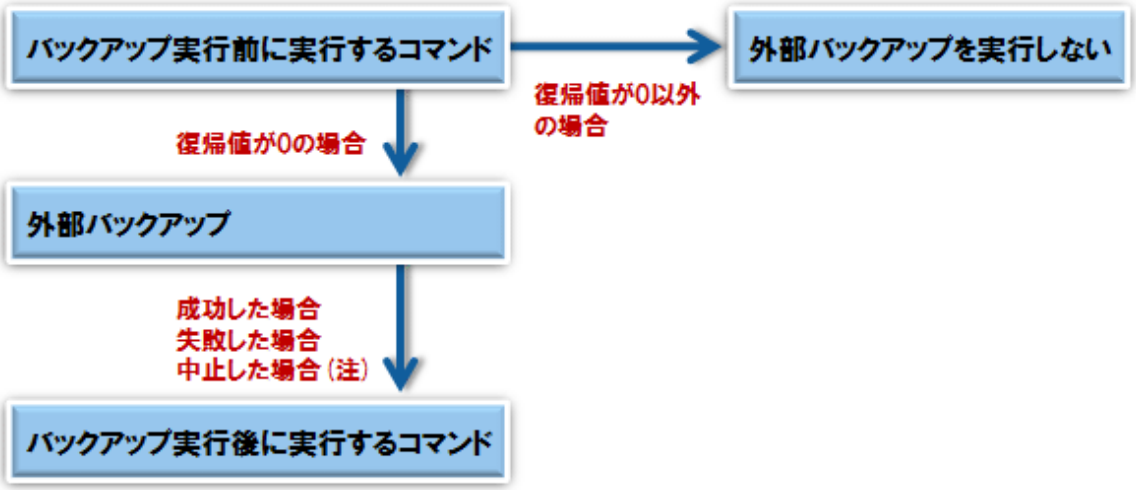
```
    exit $?
fi
```

(1)、(2)で、/opt/FJSVaplamdb/bin/apl_postbackup_from_StorageUnit.shに渡す引数は、以下のとおりです。

状況	引数
外部バックアップに成功した場合	0
外部バックアップに失敗した場合	1

参考

外部バックアップ実行前に実行するコマンドが失敗した場合の動作や、外部バックアップに失敗した場合に、外部バックアップ実行後に実行するコマンドが実行されるかどうかは、バックアップ製品によって異なります。以下の条件を満たすように、バックアップ製品側で設定してください。



注）バックアップ製品によっては、バックアップジョブを中止した場合、バックアップ実行後に実行するコマンドが自動では実行されません。

そのときは、バックアップジョブを中止したServerUnitにおいて、手動で以下のコマンドを実行してください。

/opt/FJSVaplamdb/bin/apl_postbackup_from_StorageUnit.sh 1

外部バックアップ運用時の注意

外部バックアップ運用時の注意事項について説明します。

- HA Database Readyが以下の状態の場合、外部バックアップが実行できないことがあります。
  - ー ストレージに異常が発生している場合
  - ー Native SQLインターフェースで、一方のサーバに異常が発生している場合、または、DB管理モード中の場合
  - ー Open SQLインターフェースで、両方のサーバに異常が発生している場合
- 外部バックアップ実行中には、以下の操作は実行できません。
  - ー リカバリー
  - ー バックアップ

ー 容量追加の[領域再構成]ボタンの操作

上記のいずれかの操作を実施する場合には、外部バックアップを中止してください。

- 外部バックアップ実行中に以下の操作を実行すると、外部バックアップが失敗します。

  ー シャットダウン

  ー 修正適用

  ー 修正削除

  ー BIOS/ファームウェアの更新

  ー ハードウェア部品交換

  ー ネットワークの変更

  ー 管理ネットワークの経路設定

  上記のいずれかの操作を実施する場合には、外部バックアップを中止してください。

- Open SQLインターフェースの場合には、片方のサーバだけでバックアップを取得すればよいため、ServerUnit#1またはServerUnit#2のいずれかでバックアップ実行前に実行するコマンドが失敗しますが、問題はありません。

- Appliance Managerに「外部バックアップに失敗しました。」のメッセージが表示された場合、または、バックアップ製品にエラーが出力されている場合は、外部バックアップに失敗しています。以下の手順で対処を実施してください。

  1. Appliance Managerの対処ウィンドウに表示されている対処方法、または、バックアップ製品のドキュメントに従って対処を実施する。
  2. 外部のバックアップ媒体上に取得したバックアップを破棄する。
  3. 再度“表D.1 バックアップジョブの一覧”で示すServerUnit#1およびServerUnit#2のバックアップジョブを作成し、実行する。その際、ServerUnit#1とServerUnit#2のバックアップジョブの開始時刻は同一にする。

- 外部バックアップが失敗した場合に、バックアップを途中から再開する機能は使用しないでください。

- リカバリーボタンによるリカバリー、または、外部バックアップを用いたリカバリーを実施した後は、必ずHA Database Readyのバックアップを実施してから外部バックアップを実行してください。HA Database Readyのバックアップを実施する前に外部バックアップを実行した場合、この外部バックアップのデータがリカバリー実施以前のデータとなっている可能性があり、この外部バックアップのデータでは目標の復旧時点を保証できません。

- 外部バックアップを多重実行する運用や、外部バックアップ時間が24時間以上となるような運用は行わないでください。

- 外部バックアップを用いてリカバリーを行う場合、最後にHA Database Readyのバックアップが完了した時点にリカバリーされます。ただし、HA Database Readyのバックアップが完了してから「バックアップを終了しました。」のメッセージが出力されるまでの間には、タイムラグがあり、その間に発生したトランザクションは保証されません。

- バックアップ開始時点にリカバリーしたい場合は、HA Database Readyのバックアップの開始から終了まで、業務を停止してください。

D.6.2　外部バックアップを用いたリカバリー

外部バックアップを用いたリカバリーは、以下の手順で実施します。
以下の準備を実施することで、指定した時刻にリカバリーが一度だけ実行されます。

1. アプリケーションの停止や、利用者へ停止をアナウンスします。
2. 被災などでHA Database Readyのサーバおよびストレージが破壊されてしまった場合には、以下の操作を実施します。
   a. “3.6.4 ハードウェア部品交換”に従い、ハードウェアの部品交換を行います。この際、“交換した装置の起動”では、“データベースを復旧せずにデータベースインターフェースの初期化を行う場合”の方法を実施してください。
   b. データベースインターフェース、データベースの文字コード、ポート番号については、初期化前と同一の値を指定してください。
   c. Native SQLインターフェースの場合、[手動バックアップ]ボタンによりバックアップを実施します。
3. Appliance Managerにエラーメッセージが出力されている場合は、“3.4 警告・異常時の対処とリカバリー”に従い対処します。
4. Open SQLインターフェース使用時で、格納データの暗号化を設定している場合は、以下の作業を実施します。
   なお、本作業ではサーバユニットに管理用のユーザーIDでログインする必要があります。サーバユニットへログイン方法については、“付録G サーバへのログイン方法”を参照してください。ただし、接続時のユーザーIDはrootではなく、管理用のユーザーIDを指定してください。
   a. キーストアをリストアします。
      両方のサーバユニット(ServerUnit#1およびServerUnit#2)に管理用のユーザーIDでログインし、バックアップ済のキーストアをscpコマンド、sftpコマンドなどを利用して、リストアします。本作業は、両方のサーバユニットに対して行ってください。

```
scp  -p鍵管理サーバ用ID@鍵管理サーバのIPアドレス:/work/keystore_20131201.ks(注) /var/pg_keystore/location/
keystore.ks
```

      注) リストアするバックアップデータに対応したキーストアをリストアする必要があります。対応関係については“D.8.3 バックアップ”を参照してください。
   b. ファイルの所有者の変更とキーストアの自動オープンの有効化を実施します。
      pgx_keystoreコマンドを実行し、キーストアの自動オープンを有効にしてください。本作業は、両方のサーバユニットに対して行ってください。

```
# chown 管理用ユーザーID /var/pg_keystore/location/keystore.ks
# pgx_keystore --enable-auto-open /var/pg_keystore/location/keystore.ks
パスフレーズを入力してください:
キーストアの自動オープンが有効になりました
```

5. バックアップ製品にリストアジョブを登録します。
   バックアップ製品には、リストアジョブという機能があり、外部バックアップからHA Database Readyのストレージにリストアを実行できます。また、リストア実行後に実行するコマンドを登録することにより、前回HA Database Readyのバックアップが完了した時点までデータベースを復旧できます。リストアジョブは、ServerUnit#1とServerUnit#2のそれぞれに登録します。リストアジョブでは、以下の設定を行います。
   a. リストアジョブのスケジュールを登録
      リストアジョブは一度だけ実行されるように設定します。また、ServerUnit#1のリストアジョブと、ServerUnit#2のリストアジョブが同時刻に開始するように設定します。
   b. リストア対象のディレクトリを登録
      それぞれのリストアジョブがリストアするディレクトリとして、以下のディレクトリを登録します。

表D.2 リストアジョブの一覧

データベースインターフェース	リストアジョブ	リストア元（外部バックアップ媒体上）	リストア先
Open SQL	ServerUnit#1のジョブ	共通のバックアップ先	ServerUnit#1上の以下2つ。 ・/disk1/pg/archived_xlog/ ・/disk2/pg/
	ServerUnit#2のジョブ		ServerUnit#2上の以下2つ。 ・/disk1/pg/archived_xlog/ ・/disk2/pg/
Native SQL	ServerUnit#1のジョブ	ServerUnit#1用のバックアップ先	ServerUnit#1上の以下2つ。 ・/disk2/rdb/backup/ ・/disk4/rdb/cntl_back/
	ServerUnit#2のジョブ	ServerUnit#2用のバックアップ先	ServerUnit#2上の以下2つ。 ・/disk2/rdb/backup/ ・/disk4/rdb/cntl_back/

c. リストア実行前とリストア実行後に実行するコマンドを登録
以下のコマンドをバックアップ製品からアクセスできるディレクトリにコピーし、リストアジョブに登録します。

状況	コマンド名
リストア実行前に実行するコマンド	/opt/FJSVaplamdb/bin/apl_prerestore_to_StorageUnit.sh
リストア実行後に実行するコマンド(注)	/opt/FJSVaplamdb/bin/apl_postrestore_to_StorageUnit.sh

注) バックアップ製品ごとにカスタマイズすることを推奨します。

例

バックアップ製品でエラーが発生した際にAppliance Managerにメッセージを表示する場合

「リストア実行後に実行するコマンド」をカスタマイズすることで、リストア中にバックアップ製品でエラーが発生した場合に、Appliance Managerのメッセージウィンドウに「外部バックアップからのリストアが失敗しました。」のメッセージを出力させることができます。
この場合、以下の条件を満たすコマンドを作成し、バックアップ製品からアクセスできるディレクトリに置いて実行権を付けた後、リストアジョブに登録します。

リストア実行後に実行するコマンドの例(NetVault Backup使用時)を以下に示します。

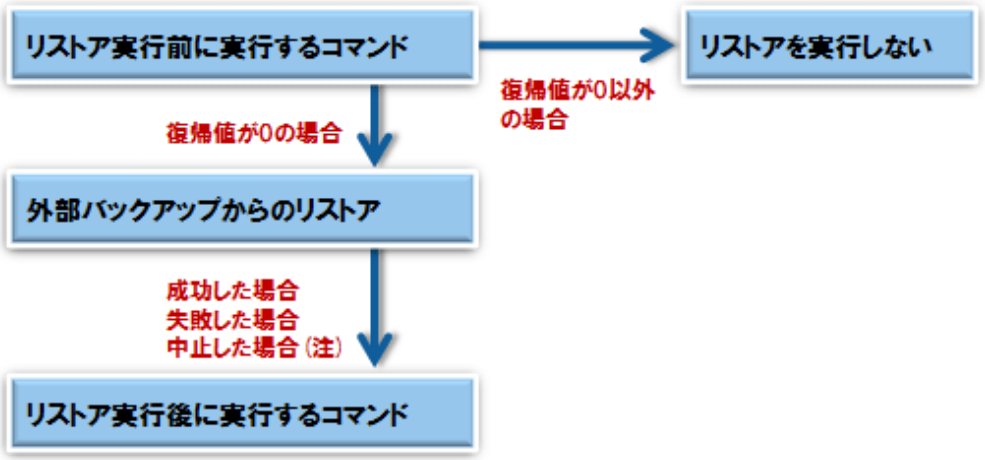
```
#!/bin/bash

if [ "${NV_STATUS}" = "FAILED" ] ; then
      /opt/FJSVaplamdb/bin/apl_postrestore_to_StorageUnit.sh 1    …(1)
      exit $?
else
      /opt/FJSVaplamdb/bin/apl_postrestore_to_StorageUnit.sh 0    …(2)
      exit $?
fi
```

(1)、(2)で、/opt/FJSVaplamdb/bin/apl_postrestore_to_StorageUnit.shに渡す引数は、以下のとおりです。

状況	引数
外部バックアップからのリストアに成功した場合	0
外部バックアップからのリストアに失敗した場合	1

参考

リストア実行前に実行するコマンドが失敗した場合の動作や、リストアに失敗した場合にリストア実行後に実行するコマンドが実行されるかどうかは、バックアップ製品によって異なります。以下の条件を満たすように、バックアップ製品で設定を行ってください。



注)バックアップ製品によっては、リストアジョブを中止した場合、リストア実行後に実行するコマンドが自動では実行されません。

そのときは、リストアジョブを中止したServerUnitにおいて、手動で以下のコマンドを実行してください。

/opt/FJSVaplamdb/bin/apl_postrestore_to_StorageUnit.sh 1

外部バックアップを用いたリカバリー運用時の注意

外部バックアップを用いたリカバリー運用時の注意事項について説明します。

- リストア中にAppliance Managerに以下のメッセージが出力される場合がありますが、問題はありません。
  - 二重化したデータベースの一方が停止しました。
  - データベースサービスが停止しました。
  - 切り替えに失敗しました。
- Open SQLインターフェースの場合には、片方のサーバだけでリストアを実行すればよいため、ServerUnit#1またはServerUnit#2のいずれかでリストア実行前に実行するコマンドが失敗しますが、問題はありません。
- Appliance Managerのメッセージウィンドウに、「業務が開始できるようになりました。引き続きリカバリーを継続します。」が表示された時点で、業務が再開できます。
- Appliance Managerに「外部バックアップからのリストアが失敗しました。」のメッセージが表示された場合、または、バックアップ製品にエラーが出力されている場合は、外部バックアップを用いたリカバリーに失敗しています。以下の手順で対処を実施してください。
  1. Appliance Managerの対処ウィンドウに表示されている対処方法、または、バックアップ製品のドキュメントに従って対処する。
  2. 再度“表D.2 リストアジョブの一覧”で示すServerUnit#1およびServerUnit#2のリストアジョブを作成し、実行する。そのとき、ServerUnit#1とServerUnit#2のリストアジョブの開始時刻は同一にする。

D.7　ホスト名の変更

HA Database Readyのホスト名を変更する場合は、以下の手順で実施してください。

注意

- ホスト名の変更作業では、HA Database Readyのサーバの再起動を伴います。
  そのため、実行する前にアプリケーションの停止や利用者へのアナウンスを行ってください。
- ホスト名の変更は、セットアップの完了後に実行してください。セットアップが完了していない状態でホスト名の変更を実施した場合に、正常に動作しない可能性があります。
- ホスト名の変更は、実行から完了まで約10分かかります。

1. ホスト名の変更を実行する前に、アプリケーションの停止や利用者へのアナウンスをします。
2. いずれかのサーバユニットに、スーパーユーザーでログインします。ログイン方法については、“付録G サーバへのログイン方法”を参照してください。
3. 以下に示すコマンドを実行し、ホスト名を変更します。

```
# /opt/FJSVaplamdb/bin/modify_hostname.sh
```

4. コマンドを実行すると、以下の項目の入力を求められます。
   a. ServerUnit#1のホスト名
   b. ServerUnit#2のホスト名

   入力後に、ホスト名の変更処理が実行されます。“Hostname modifications have been completed.”のメッセージが表示された後に、サーバが再起動されます。

   以下に、コマンドの実行例を示します。**太字**は、お客様が入力する項目です。

```
# /opt/FJSVaplamdb/bin/modify_hostname.sh

Input new hostname of ServerUnit#1.(Current hostname = aphost1)
> newhost1                                          …a.ServerUnit#1のホスト名

Input new hostname of ServerUnit#2.(Current hostname = aphost2)
> newhost2                                          …b.ServerUnit#2のホスト名

Type "OK" to update the hostnames.
Type "exit" to cancel.

[ Hostname settings ]
1) ServerUnit#1 : aphost1 -> newhost1
2) ServerUnit#2 : aphost2 -> newhost2

(OK/exit[exit])> OK

**********
Hostname modifications have been completed.
```

5. サーバの再起動後に、ホスト名が変更されていることを確認してください。
   ホスト名を確認するためには、ServerUnit#1およびServerUnit#2にスーパーユーザーでログインし、以下のコマンドを実行してください。

```
# hostname
```

注意

ー ホスト名は下記の命名規約に従う必要があります。

- ASCII文字のaからzまでの英字と0から9までの数字と-(ハイフン)を使用してください。
- 1～63文字以内で構成してください。
- ホスト名の最初と最後に-(ハイフン)を使用することはできません。

ー ホスト名を変更した場合は、管理端末の名前解決設定を変更してください。管理端末の名前解決については“3.1 管理端末の設定”を参照してください。

ー Open SQLインターフェース使用時で、格納データの暗号化を設定している場合は、以下の作業を実施する必要があります。
初期値以外のパスフレーズを使用している場合、5.サーバの再起動後に、Appliance Managerに「データベースサービスが停止しました。」のメッセージが表示され、Appliance Managerの稼働状態が異常になります。このときは、以下の手順を実施してください。

a. キーストアの自動オープンの有効化を実施します。
この作業は、サーバユニットに、管理用のユーザーIDでログインして実施します。本作業は、両方のサーバユニットに対して行ってください。

```
# pgx_keystore --enable-auto-open /var/pg_keystore/location/keystore.ks
パスフレーズを入力してください:
キーストアの自動オープンが有効になりました
```

b. HA Database Readyをシャットダウンします。

c. 電源を投入します。

参考

HA Database Readyのホスト名を変更しても、運用管理サーバによる監視に影響はありません。

ただし、“E.1 運用監視”で設定した[運用管理サーバで表示するホスト名]にHA Database Readyのホスト名に合わせた名を指定している場合は、ここで変更したHA Database Readyのホスト名に合わせて、[運用管理サーバで表示するホスト名]も変更することをお勧めします。
[運用管理サーバで表示するホスト名]を変更したときは、Systemwalker Centric Managerの設定も変更する必要があります。

[運用管理サーバで表示するホスト名]を変更したい場合は、“E.1 運用監視”を参照してください。
Systemwalker Centric Managerの設定変更は、“F.1 運用準備”を参照してください。

D.8　格納データの暗号化

格納データを暗号化する場合は、以下の手順で実施してください。

ポイント

- 本機能は、データベースインターフェースとしてOpen SQLインターフェースを選択した場合だけ利用できます。
- HA Database Readyでの格納データの暗号化は、Symfoware Serverの機能を使って実現しています。機能の詳細については、“Symfoware Server 運用ガイド”の“透過的データ暗号化による格納データの保護”をお読みください。ただし、HA Database ReadyでOpen SQLを使用する場合、使用できないSymfoware Serverの機能があります。制約機能の詳細については、“業務開発ガイド(Open SQL編)”の“HA Database Readyでの使用制約”を参照してください。
- 本節の内容は、クライアントでの操作を伴いますので、データベース管理者とご一緒にお読みください。

D.8.1　暗号化の事前準備

格納データの暗号化の機能を使ってデータベースを暗号化するためには、以下の準備が必要です。

鍵管理サーバの準備

キーストアをバックアップするための鍵管理サーバを用意する必要があります。鍵管理サーバの配置場所については“1.1.2 システム構成”を参照してください。

キーストアの格納場所

キーストアを格納するディレクトリは、"/var/pg_keystore/location"です。

パスフレーズの初期値

キーストアのパスフレーズの初期値は、"DATABASEREADY"です。

クライアントでの操作

格納データの暗号化では、HA Database Readyのサーバ側で実施する作業とアプリケーションサーバ側のクライアントで実施する作業があります。以降の手順のなかで、クライアントで実施する作業には、“クライアントでの操作”と明記しています。なお、クライアントでの操作の場合も、“2.2.2 管理用のユーザーIDの設定”で作成した管理用のユーザーIDを利用してください。“業務開発ガイド(Open SQL編)”の“データベースを作成するユーザーの作成”で作成したユーザーIDでは操作できませんので、注意してください。

クライアントからpsqlコマンドを使用し、SQL文を発行する例を以下に示します。本節では以下の例を使用して説明します。

指定例

```
$ psql -d postgres  -h 192.168.0.1,192.168.0.2  -p 26500 -U manager  -c ”SQL文”        (注1)
または
$ psql -d postgres  -h 192.168.0.1,192.168.0.2  -p 26500 -U manager  -f /data/xxx.txt
```

postgres：データベース名
192.168.0.1,192.168.0.2：業務用のIPアドレス
26500：ポート番号
manager : 管理用のユーザーID
SQL文 : 実行したいSQL文
/data/xxx.txt：SQL文を記述した入力ファイル名(注2)

注1)パスフレーズなどの値変更を行う場合は、パスフレーズの漏えい防止のため、この方法で実行してください。
注2) LinuxまたはSolarisで実行する際の指定方法です。Windowsの場合は、パスの区切りに¥を使用し、d:のようにドライブの指定が必要です。

入力ファイル(/data/xxx.txt)の記述例

```
SELECT  ...;
```

クライアントでの操作方法の詳細については、“業務開発ガイド(Open SQL編)”を参照してください。

D.8.2　暗号化の設定

HA Database Readyの格納データの暗号化は、キーストアのパスフレーズを変更することで利用できます。格納データの暗号化を利用するには、以下の手順で設定します。

注意

管理者はAppliance Managerの[ホーム]画面の稼働状態が「正常」になっていることを確認してから本作業を進め、暗号化の設定作業がクライアントで実施されている間、Appliance Managerの[ホーム]画面の稼働状態を監視してください。

作業中にAppliance Managerの稼働状態が「警告」になった場合は、“D.8.3 バックアップ”と“D.8.4 リカバリー”の手順が複雑になるので、注意してください。

1. キーストアのパスフレーズを変更します。(クライアントでの操作)
   管理用のユーザーIDにて、クライアントからpsqlコマンドを実行して以下のSQL文を発行します。

   指定例

   ```
   $ psql -d postgres  -h 192.168.0.1,192.168.0.2  -p 26500  -U manager -c "SELECT
   pgx_set_keystore_passphrase('DATABASEREADY', 'new_passphrase')"
   ```

   “DATABASEREADY”はパスフレーズの初期値です。
   new_passphraseには、新しいパスフレーズを指定してください。値については“Symfoware Server 運用ガイド”の“透過的データ暗号化制御関数”を参照してください。

2. テーブル空間の暗号化を設定します。(クライアントでの操作)
   管理用のユーザーIDにて、クライアントからpsqlコマンドを実行して、テーブル空間の暗号化を行います。

   指定例

   ```
   $ psql -d postgres  -h 192.168.0.1,192.168.0.2  -p 26500  -U manager -f /data/tbl_encrypt.txt
   ```

   入力ファイル(/data/tbl_encrypt.txt)の記載例：以降に作成するテーブル空間の暗号化アルゴリズムを指定

   ```
   SET tablespace_encryption_algorithm = 'AES256';
   CREATE TABLESPACE secure_tablespace LOCATION …
   ```

   入力ファイル(/data/tbl_encrypt.txt)の記載例：以降に作成するテーブル空間は暗号化しないように指定

   ```
   SET tablespace_encryption_algorithm = 'none';
   ```

   ポイント

   CREATE TABLESPACE文を使用しない方法

   CREATE TABLESPACE文を使用せずに、CREATE TABLE文を実行する利用者に対しては、暗号化されたTABLESPACE名を公開し、default_tablespaceを設定させるように運用してください。

   ```
   SET default_tablespace  = secure_tablespace;
   ```

3. 暗号化されているテーブル空間を確認します。(クライアントでの操作)
   管理用のユーザーIDにて、クライアントからpsqlコマンド実行してテーブル空間が暗号化されているかを確認してください。確認方法については、“Symfoware Server 運用ガイド”の“ 暗号化されているテーブル空間の確認”を参照してください。

4. キーストアおよびデータベースのバックアップを実施してください。詳細は、“D.8.3 バックアップ”を参照してください。

D.8.3 バックアップ

暗号化の設定、マスタ暗号化キーの変更、またはキーストアのパスフレーズの変更を行ったあとは、ハードウェア障害などに備えて、必ずキーストアとデータベースのバックアップを実施してください。本バックアップデータは、以下の場合に使用します。

- システムディスクの二重障害からの復旧する場合
- 外部バックアップを用いてバックアップ時点に復旧する場合

注意

キーストアのバックアップデータを紛失すると、データベースを復旧できなくなるので注意してください。

バックアップ作業では、サーバユニットにログインする必要があります。ログイン方法については、“付録G サーバへのログイン方法”を参照してください。ただし、接続時のユーザーIDはrootではなく、管理用のユーザーIDを指定してください。

1. キーストアをバックアップします。
   暗号化の設定、マスタ暗号化キーの変更、またはキーストアのパスフレーズの変更を実施した場合(ここでは各作業をまとめて、暗号化作業、と略します)の、Appliance Managerの[ホーム画面]の稼働状態によって、バックアップの手順が異なります。

   ー 暗号化作業中にAppliance Managerの稼働状態が「正常」の場合

   いずれかのサーバユニット(ServerUnit#1またはServerUnit#2)に管理用のユーザーIDでログインし、scpコマンド、またはsftpコマンドなどを利用して、鍵管理サーバにキーストアをバックアップします。
   バックアップの際には、ファイルの実行権限を引き継ぐようにしてください。

   指定例

   ```
   # scp -p /var/pg_keystore/location/keystore.ks  鍵管理サーバ用ID@鍵管理サーバのIPアドレス:/work/
   keystore_20131201.ks
   ```

   ー 暗号化作業の途中でAppliance Managerの稼働状態が「警告」になった場合
   両方のサーバユニット(ServerUnit#1およびServerUnit#2)のキーストアのうち、新しい方のキーストアをバックアップする必要があります(同一日時の場合どちらでも可)。そのため、両方のサーバユニットに管理用のユーザーIDでログインし、scpコマンド、またはsftpコマンドなどを利用して、鍵管理サーバに新しい方のキーストアをバックアップします。
   バックアップの際には、ファイルの実行権限を引き継ぐようにしてください。

   サーバユニット1のキーストアを確認

   ```
   # ls -l /var/pg_keystore/location/keystore.ks
   -rw------- 1 manager manager 928 11月  1 12:00 2013 /var/pg_keystore/location/keystore.ks
   ```

   サーバユニット2のキーストアを確認

   ```
   # ls -l /var/pg_keystore/location/keystore.ks
   -rw------- 1 manager manager 928 12月  1 12:00 2013 /var/pg_keystore/location/keystore.ks
   ```

   サーバユニット2の方が新しいと判明。

   設定例(サーバユニット2のキーストアをバックアップ)

   ```
   # scp -p /var/pg_keystore/location/keystore.ks  鍵管理サーバ用ID@鍵管理サーバのIPアドレス:/work/
   keystore_20131201.ks
   ```

2. データベースをバックアップします。
   キーストアのバックアップを行うと同時に、データの整合性を保つため、Appliance Managerを使ってデータベースのバックアップを実施してください。
   データベースのバックアップについては、“3.5.2 バックアップ”を参照してください。

注意

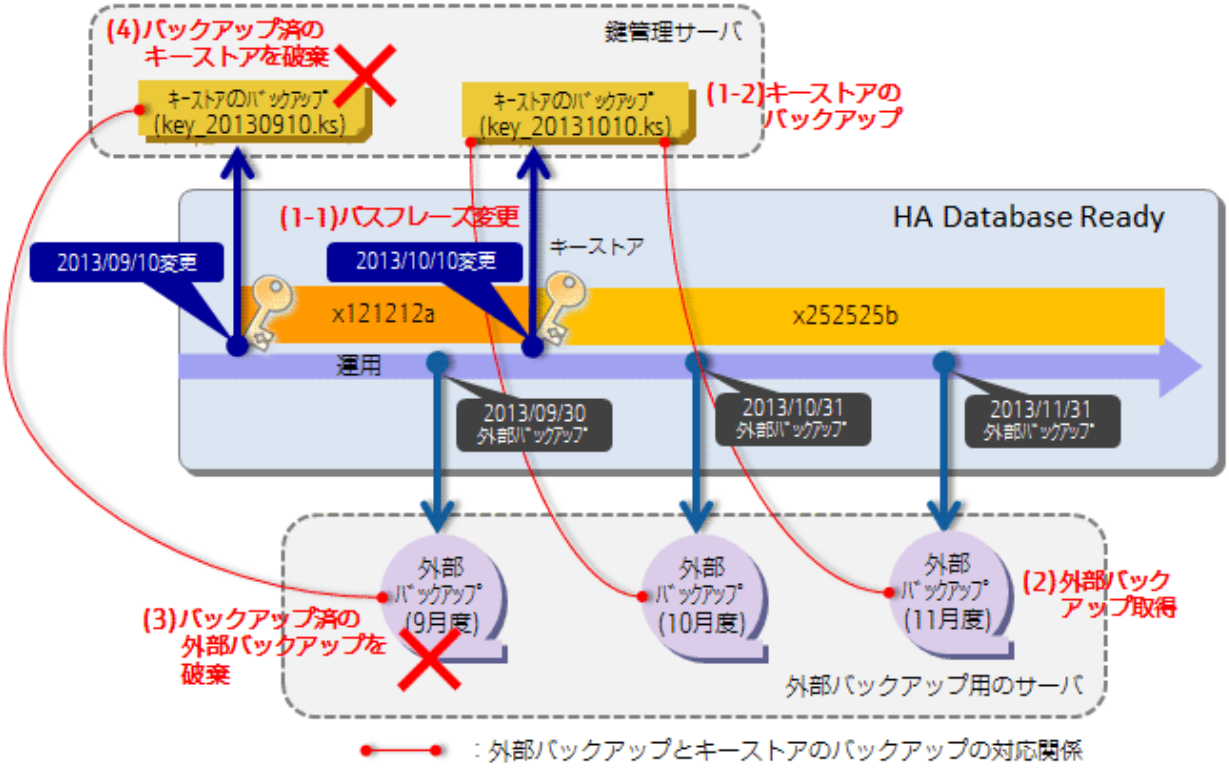
マスタ暗号化キーの変更、またはキーストアのパスフレーズの変更を行った場合は、キーストアのバックアップを実施する必要があります。すでにバックアップ済のキーストアについては、以下の契機で破棄してください。

・ 自動バックアップ（手動バックアップ）の場合

マスタ暗号化キーの変更、またはキーストアのパスフレーズの変更後に、自動バックアップ(手動バックアップ)が完了した後に、バックアップ済のキーストアを破棄してください。

・ 外部バックアップの場合

マスタ暗号化キーの変更、またはキーストアのパスフレーズの変更(1-1)およびキーストアのバックアップ(1-2)後に、外部バックアップが成功(2)し、かつ、すでにバックアップ済の外部バックアップデータを破棄するとき(3)に、バックアップ済のキーストアを破棄してください(4)。以下の図に例を示します。



D.8.4　リカバリー

ハードウェア障害などが発生した際の、以下のリカバリー方法について説明します。

・ 外部バックアップを用いてバックアップ時点にデータベースの復旧する場合

・ リカバリーボタンを用いてデータベースを復旧する場合

外部バックアップを用いてバックアップ時点にデータベースの復旧する場合

最初にキーストアのリストアを実施する必要があります。詳細は、“D.6.2 外部バックアップを用いたリカバリー”を参照してください。

リカバリーボタンを用いてデータベースを復旧する場合

暗号化の設定、マスタ暗号化キーの変更、キーストアのパスフレーズの変更を実施した場合(ここでは各作業をまとめて、暗号化作業、と略します)の、Appliance Managerの[ホーム画面]の稼働状態によって、リカバリーの手順が異なります。

・ 暗号化作業中にAppliance Managerの稼働状態が「正常」の場合は、リカバリーボタンを押してリカバリーを実行します。

・ 暗号化作業の途中でAppliance Managerの稼働状態が「警告」になった場合は、以下の手順が必要です。

以下の作業ではサーバユニットに管理用のユーザーIDでログインする必要があります。サーバユニットへログイン方法については、“付録G サーバへのログイン方法”を参照してください。ただし、接続時のユーザーIDはrootではなく、管理用のユーザーIDを指定してください。

1. キーストアをリストアします。
両方のサーバユニット(ServerUnit#1およびServerUnit#2)に管理用のユーザーIDでログインし、バックアップ済のキーストアをscpコマンド、sftpコマンドなどを利用して、リストアします。本作業は、両方のサーバユニットに対して行ってください。

```
scp  -p鍵管理サーバ用ID@鍵管理サーバのIPアドレス:/work/keystore_20131201.ks(注) /var/pg_keystore/location/
keystore.ks
```

注) 最新のキーストアをリストアする必要があります。

2. ファイルの所有者の変更とキーストアの自動オープンの有効化を実施します。
pgx_keystoreコマンドを実行し、キーストアの自動オープンを有効にしてください。本作業は、両方のサーバユニットに対して行ってください。

```
# chown 管理用ユーザーID /var/pg_keystore/location/keystore.ks
# pgx_keystore --enable-auto-open /var/pg_keystore/location/keystore.ks
パスフレーズを入力してください:
キーストアの自動オープンが有効になりました
```

3. リカバリーボタンを押して、リカバリーを実行します。

注意

ー 上記の手順1,2を実施せずにリカバリーボタンを実施した場合、Appliance Managerのメッセージウィンドウに11013「リカバリーに失敗しました。」または11001「二重化したデータベースの一方が停止しました。」が表示されます。この場合は、再度上記の手順1.から実施しなおしてください。

ー 上記の手順1,2は、暗号化の設定、マスタ暗号化キーの変更または、キーストアのパスフレーズの変更を実施したあとの、初回のリカバリー実行時だけ実施します。上記の手順でリカバリーした後、マスタ暗号化キーの変更またはキーストアのパスフレーズの変更はせずに再度リカバリーが必要になった場合は、リカバリーボタンを押す(上記の手順3)だけで復旧できます。

D.8.5 マスタ暗号化キーの変更

同じ暗号化キーを長期間使い続けることは、攻撃者に対して暗号データの解読の機会を与えてしまいます。一定期間ごと、またはキーが危険にさらされたときには、以下の手順でキーを変更することを薦めます。

注意

管理者はAppliance Managerの[ホーム]画面の稼働状態が「正常」になっていることを確認してから本作業を進め、暗号化の設定作業がクライアントで実施されている間、Appliance Managerの[ホーム]画面の稼働状態を監視してください。

作業中にAppliance Managerの稼働状態が「警告」になった場合は、“D.8.3 バックアップ”と“D.8.4 リカバリー”の手順が複雑になるので、注意してください。

1. マスタ暗号化キーを変更します。(クライアントでの操作)
管理用のユーザーIDにて、クライアントからpsqlコマンドを実行して以下のSQL文を発行します。

指定例

```
$ psql -d postgres  -h 192.168.0.1,192.168.0.2  -p 26500  -U manager -c "SELECT pgx_set_master_key('passphrase')"
```

passphraseには、パスフレーズを指定してください。

2. ハードウェア障害などに備えて、キーストアおよびデータベースのバックアップを実施してください。詳細は、“D.8.3 バックアップ”を参照してください。

D.8.6 キーストアのパスフレーズの変更

組織のセキュリティ・ポリシーでは通常、パスフレーズを知るセキュリティ管理者が異動や退職で職務から外れるときには、パスフレーズを変更することが求められます。また、万一ソーシャル・エンジニアリングのような手口でパスフレーズが危険にさらされたときには、以下の手順でパスフレーズを変更することをお薦めします。

注意

管理者はAppliance Managerの[ホーム]画面の稼働状態が「正常」になっていることを確認してから本作業を進め、暗号化の設定作業がクライアントで実施されている間、Appliance Managerの[ホーム]画面の稼働状態を監視してください。

作業中にAppliance Managerの稼働状態が「警告」になった場合は、“D.8.3 バックアップ”と“D.8.4 リカバリー”の手順が複雑になるので、注意してください。

1. キーストアのパスフレーズを変更します。(クライアントでの操作)
   管理用のユーザーIDにて、クライアントからpsqlコマンドを実行して以下のSQL文を発行します。

   指定例

   ```
   $ psql -d postgres  -h 192.168.0.1,192.168.0.2  -p 26500  -U manager -c "SELECT
   pgx_set_keystore_passphrase('old_passphrase', 'new_passphrase')"
   ```

   old_passphraseには現在のパスフレーズを、new_passphraseには新しいパスフレーズを指定してください。値については“Symfoware Server 運用ガイド”の“透過的データ暗号化制御関数”を参照してください。

2. ハードウェア障害などに備えて、キーストアおよびデータベースのバックアップを実施してください。詳細は、“D.8.3 バックアップ”を参照してください。

付録E　運用管理サーバとの連携

運用管理サーバとの連携について説明します。

やりたいこと	参照先
他のサーバと一括して運用状態を監視したい(注1)	“E.1 運用監視”
お客様のNTPサーバと時刻同期したい(注2)	“E.2 時刻補正”
システムの稼働状態をメールで受け取りたい	“E.3 メール通知”
Interstage Charset Managerが管理している文字資源を活用したい(注3)	“E.4 文字管理”
リモートから電源を投入したい	“E.5.1 電源の投入”

注1) 警告や異常を検出した場合の対処は、Appliance Managerで行ってください。
注2) HA Database Readyを構成する装置は同一の時刻を示すように設定されています。
注3) データベースインターフェースとしてNative SQLインターフェースを選択した場合に有効です。

E.1　運用監視

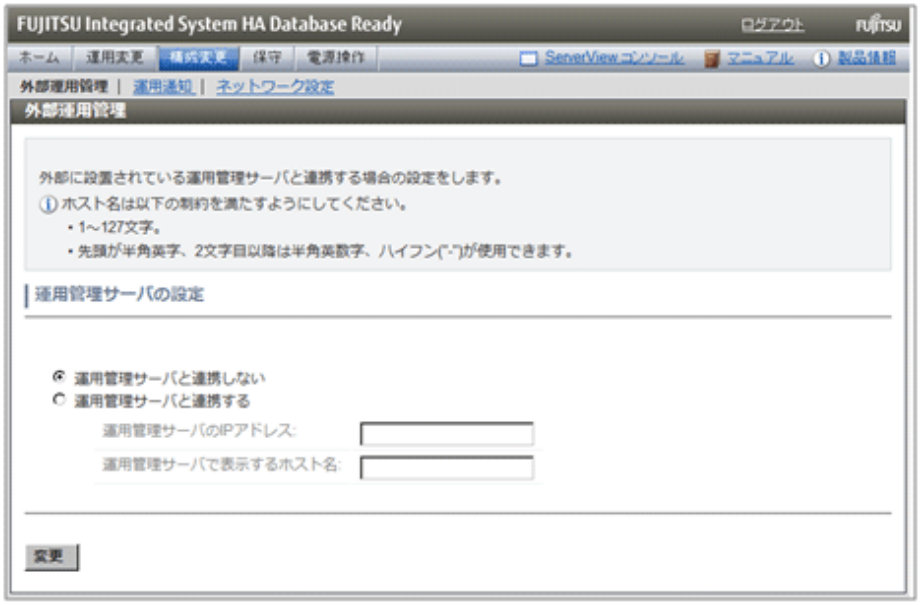
HA Database Readyは、外部に設置された運用管理サーバと連携できます。

HA Database Readyと連携できる運用管理システムで必要なソフトウェアは以下です。

- Systemwalker Centric Manager Enterprise Edition V13.6(マネージャー)
- Systemwalker Centric Manager Standard Edition V13.6(マネージャー)

外部に設置された運用管理サーバとの連携を設定する場合は、以下の手順で行います。

1. Appliance Managerで[構成変更]を選択し、次に[外部運用管理]タブを開きます。[外部運用管理]画面が開きます。



2. [運用管理サーバの設定]の[運用管理サーバと連携する]を選択します。
3. [運用管理サーバのIPアドレス]と[運用管理サーバで表示するホスト名]を指定して、[変更]ボタンをクリックします。
[運用管理サーバで表示するホスト名]で指定したホスト名は、末尾に、1および2を付加して、運用管理サーバへ登録されます。

ポイント

[運用管理サーバで表示するホスト名]には制約を満たす任意の文字列を指定できます。HA Database Readyのホスト名と同一にする必要はありませんが、運用管理サーバで監視している他のサーバと重複しないように指定してください。重複しなければ、HA Database Readyのホスト名に合わせて「aphost」にすることをお勧めします。HA Database Readyが2台以上存在する場合は、「m1aphost」のようにaphostの先頭に機器を識別するための文字列を付加することをお勧めします。[運用管理サーバで表示するホスト名]は以下の制約を満たすようにしてください。

- 1～127文字
- 先頭は半角英字、2文字目以降は半角英数字、ハイフン("-")が使用できます。

ポイント

運用管理サーバと連携することによって、運用管理サーバでHA Database Readyの以下のメッセージを監視できます。

- Appliance Managerのメッセージ
  Appliance Managerのメッセージについては“付録A メッセージ一覧”を参照してください。
- ServerView Operations Managerが出力するメッセージ(エラーレベルが警告・エラーのもの)

参照

- Systemwalker Centric ManagerでHA Database Readyの運用を管理する場合の基本的な設定と運用方法については、“付録F Systemwalker Centric Managerの設定と運用”を参照してください。
- 他社の運用管理製品でHA Database Readyを管理する場合、Systemwalker Centric Managerの運用管理サーバから他社の運用管理製品へSNMPトラップを通知します。
  SNMPトラップを通知する方法については、“Systemwalker Centric Manager 使用手引書 監視機能編”の“SNMPトラップを発行する”を参照してください。

E.2 時刻補正

HA Database Readyの外部のNTPサーバと、HA Database Readyの時刻を同期させたい場合は、以下の手順で設定してください。

1. ServerUnit#1に、スーパーユーザーでログインします。ログイン方法については、“付録G サーバへのログイン方法”を参照してください。
2. お客様のNTPの設定ポリシーに従って、OSのNTPデーモンの設定ファイル(/etc/ntp.conf)を編集します。
   /etc/ntp.confファイルの以下の部分について、参照するNTPサーバのIPアドレスに変更してください。
   - serverパラメタ
   - fudgeパラメタ

```
server   127.127.1.0 # local clock (注)
fudge    127.127.1.0 stratum 10 (注)
```

   注) 127.127.1.0のIPアドレスを、NTPサーバのIPアドレスに変更してください。
3. 以下のコマンドを実行し、NTPデーモンを再起動します。

```
# /etc/init.d/ntpd restart
```

4. 以下のコマンドを実行し、正しく設定されたかを確認します。

```
# ntpq -p
```

ntpqコマンドの出力結果において、「remote」の項目に表示された「*」が付いているIPアドレスが、指定したNTPサーバのIPアドレスと同じであることを確認してください。

5. ServerUnit#1からログアウトします。

注意

NTPサーバとの時刻同期設定は、ServerUnit#1に対してだけで実施してください。

HA Database Readyのすべての機器は、ServerUnit#1と同期するようにあらかじめ設定されており、この設定を前提として動作しています。したがって、ServerUnit#1以外でNTPの設定をしないでください。

参考

- HA Database Readyは、サーバとストレージで構成されています。これらの機器は、同じ時刻を示すように初期設定されています。
- NTPデーモンや、/etc/ntp.confファイルの記述方法については、OSのmanコマンドで参照できます。

```
# man ntpd
```

E.3 メール通知

HA Database Readyの外部のSMTPサーバと連携することで、システムの稼働状態を通知するメールを自動送信できます。

E.3.1 メールの設定

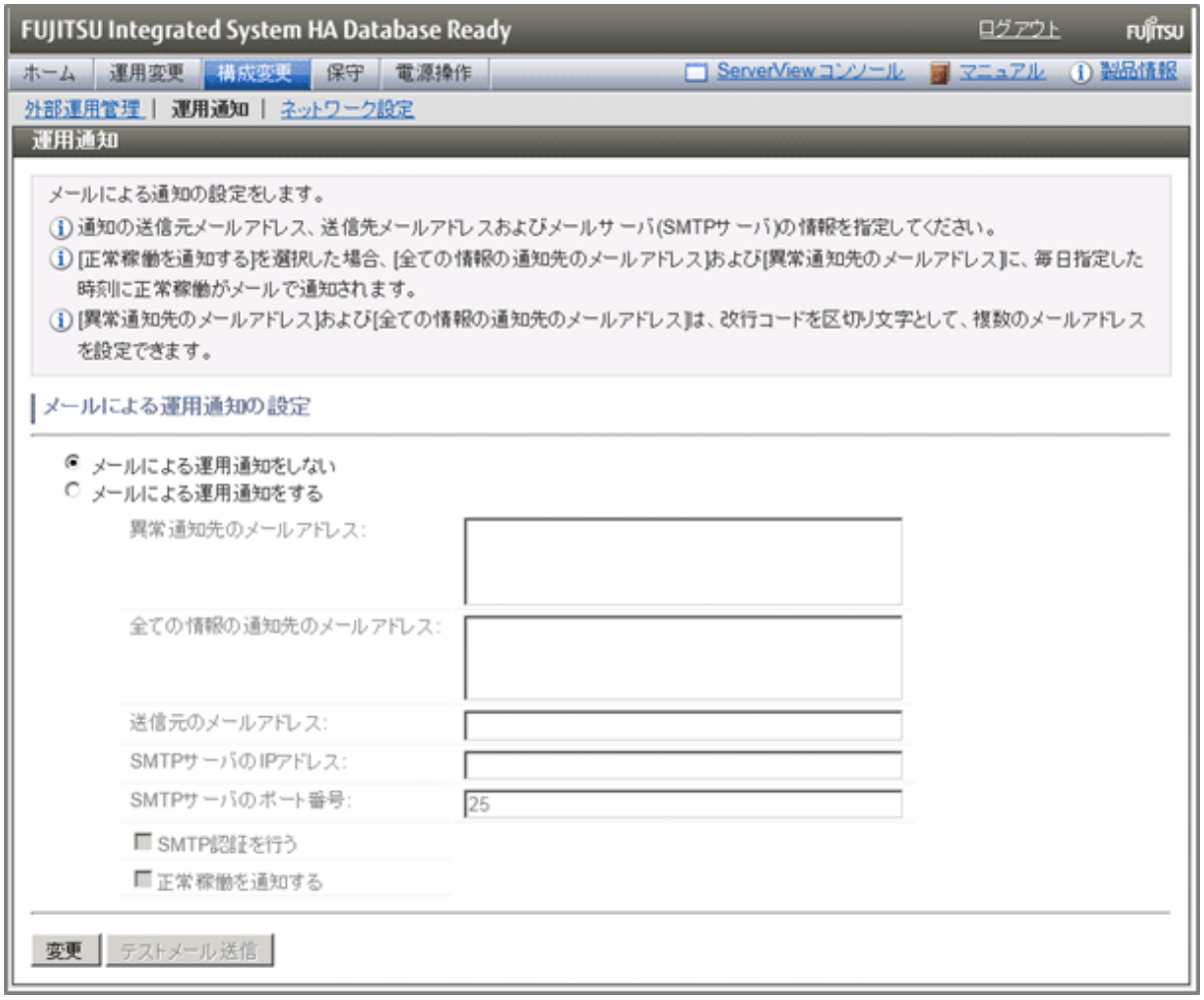
通知されるメール種別とメールアドレス設定の組合せは以下です。メールの詳細は“E.3.2 通知されるメールの内容”を参照してください。

自動送信されるメールの種別	[運用通知]画面での設定	
	[異常通知先のメールアドレス]に設定	[全ての情報の通知先のメールアドレス] に設定
データベースの警告・エラー状態の通知メール	○	○
データベース以外の警告・エラー状態の通知メール	○	○
運用情報の通知メール	ー	○
正常稼働状態の通知メール	△	△

○：自動送信される。
ー：自動送信されない。
△：[正常稼働を通知する]をチェックすると自動送信される。

メールによる稼働通知を設定する場合は、以下の手順で行います。

1. Appliance Managerで[構成変更]タブを選択し、次に[運用通知]タブを開きます。[運用通知]画面が開きます。



2. [メールによる運用通知をする]を選択します。
3. 以下の項目を設定します。
   - [異常通知先のメールアドレス]
     “A.1 FIS-HADBR_AMGRDBで始まるメッセージ”のうち、エラー種別が「警告」または「エラー」の事象が発生した場合にメールが通知されるアドレスです。
   - [全ての情報の通知先のメールアドレス]
     “A.1 FIS-HADBR_AMGRDBで始まるメッセージ”のうち、エラー種別が「情報」、「警告」または「エラー」の事象が発生した場合にメールが通知されるアドレスです。
   - [送信元のメールアドレス]
   - [SMTPサーバのIPアドレス]
   - [SMTPサーバのポート番号]

注意

[異常通知先のメールアドレス]および[全ての情報の通知先のメールアドレス]の入力規約

- 改行コード(“¥r”、“¥n”または“¥r¥n”)を区切り文字として、複数のメールアドレスを設定できます。
- 入力可能な文字数は、区切り文字を含めて1,024文字です。

ー [異常通知先のメールアドレス]と[全ての情報の通知先のメールアドレス]に同じメールアドレスを指定すると、エラーになります。

4. SMTPサーバの認証が必要な場合は、[SMTP認証を行う]をチェックして、[SMTPサーバのユーザー名]と[SMTPサーバのパスワード]を指定します。
5. 定期的に正常状態の通知を受けたい場合は、[正常稼働を通知する]をチェックし、[通知時刻]にメールの送信時刻を設定します。
6. 入力が完了したら、[テストメール送信]をクリックしてください。確認メールが正しく到着したら、[変更]をクリックします。

注意

- メール送信で使用するSMTPサーバは、HA Database Readyとは別に用意していただく必要があります。
- SMTP認証をサポートしています。
- 通知先のメールアドレスが、SMTPサーバが許可しているアドレスの形式に一致していない場合、SMTPサーバからメール送信ができないために、指定したメールアドレスではメールを受信できません。SMTPサーバ側のセキュリティの程度によって、許可するアドレスの形式やアドレス文字列が違います。許可されている形式については、SMTPサーバの管理者に問い合わせてください。

E.3.2 通知されるメールの内容

通知されるメールの内容を、以下に示します。

- データベースの警告・エラー状態の通知メール
- データベース以外の警告・エラー状態の通知メール
- 運用情報の通知メール
- 正常稼働の通知メール

データベースの警告・エラー状態の通知メール

“A.1 FIS-HADBR_AMGRDBで始まるメッセージ”のうち、エラー種別が「警告」または「エラー」の事象が発生した場合に通知されるメールは以下のとおりです。

件名(Subject)	An unexpected event has occurred at HA Database Ready.(*管理ネットワークのIPアドレス*)
送信元(From)	運用通知で設定した送信元のメールアドレス
通知先(To)	運用通知で設定した通知先のメールアドレス
メッセージ本文	An unexpected event has occurred at HA Database Ready. Access one of the following URLs, and check the status: [*Appliance ManagerのURL1*] [*Appliance ManagerのURL2*] [Trouble Information] date: [*トラブル発生日時*] message: [*トラブル発生状況を示すメッセージ*] [User Action] [*トラブルに対する対処方法*]

データベース以外の警告・エラー状態の通知メール

“A.1 FIS-HADBR_AMGRDBで始まるメッセージ”のメッセージ一覧に記載されていない警告やエラーが発生した際に通知されるメールは以下のとおりです。

件名(Subject)	An unexpected event has occurred at HA Database Ready.(*管理ネットワークのIPアドレス*)
送信元(From)	運用通知で設定した送信元のメールアドレス
通知先(To)	運用通知で設定した通知先のメールアドレス
メッセージ本文	An unexpected event has occurred at HA Database Ready. Access one of the following URLs, and check the status: [*Appliance ManagerのURL1*] [*Appliance ManagerのURL2*] [Trouble Information] date: [*トラブル発生日時*] message: [*トラブル発生状況を示すメッセージ*]

運用情報の通知メール

“A.1 FIS-HADBR_AMGRDBで始まるメッセージ”のうち、エラー種別が「情報」の事象が発生した場合に通知されるメールは以下のとおりです。

件名(Subject)	Information email from HA Database Ready.(*管理ネットワークのIPアドレス*)
送信元(From)	運用通知で設定した送信元のメールアドレス
通知先(To)	運用通知で設定した通知先メールアドレス
メッセージ本文	[Information] date: [*発生日時*] message: [*運用情報の内容を示すメッセージ*]

正常稼働の通知メール

正常稼働を通知するメールは以下のとおりです。

件名(Subject)	HA Database Ready is up and running.(*管理ネットワークのIPアドレス*)
送信元(From)	運用通知で設定した送信元のメールアドレス
通知先(To)	運用通知で設定した通知先のメールアドレス
メッセージ本文	HA Database Ready is up and running.

E.4　文字管理

HA Database Readyは、Interstage Charset Managerが管理している文字資源を活用できます。

以下の手順で、Interstage Charset Managerの文字資源を配付します。

ポイント

この設定は、データベースインターフェースとしてNative SQLインターフェースを選択した場合に有効です。

1. 文字資源の配布を実行する前に、アプリケーションの停止、および、利用者へのアナウンスを行います。
2. ServerUnit#1にスーパーユーザーでログインします。ログイン方法については、“付録G サーバへのログイン方法”を参照してください。
3. 環境変数を設定します。

```
# export LANG=ja_JP.eucJP
# export JAVA_HOME=/usr/java/jre1.7.0_51
```

4. 以下のコマンドで、Interstage Charset Manager の資源管理サーバを指定します。

```
# /etc/opt/FSUNadj/JPAGE/bin/qgfvini /S 資源管理サーバ名（注）
```

注)Interstage Charset Manager の資源管理サーバのIPアドレスを指定してください。

5. 以下のコマンドで、Interstage Charset Managerの配付デーモンを起動します。

```
# /etc/opt/FSUNadj/JPAGE/bin/hmapp/daemon/bin/qgfrjdm -start -r/etc/opt/FSUNadj/JPAGE/bin/hmapp/daemon/bin/
RestartProperty &
```

6. Interstage Charset Managerの資源管理サーバで、コード変換の定義の実行と、文字資源の配付処理を実行してください。

参照

Interstage Charset Managerの資源管理サーバでの操作方法については、“Interstage Charset Manager Standard Edition 使用手引書 日本語資源管理編”を参照してください。

7. 文字資源の配付が完了したら、以下のコマンドで、Interstage Charset Managerの配付デーモンを停止します。

```
# /etc/opt/FSUNadj/JPAGE/bin/hmapp/daemon/bin/qgfrjdm -stop
```

8. ServerUnit#1からログアウトします。
9. ServerUnit#2にスーパーユーザーでログインし、3.～8.の手順を実行します。
10. 上記作業が完了したら、利用者へ再開をアナウンスします。

ポイント

Interstage Charset Managerの資源管理サーバで文字資源が追加された場合は、文字資源の再配付が必要です。ServerUnit#1とServerUnit#2で上記の3.～7.の手順を実行してください。
ServerUnit#1とServerUnit#2への文字資源の配付方法の詳細については、“Interstage Charset Manager Standard Edition 使用手引書 日本語資源適用編”を参照してください。

E.5 電源制御

iRMCの電源制御機能を使って電源を操作できます。

E.5.1　電源の投入

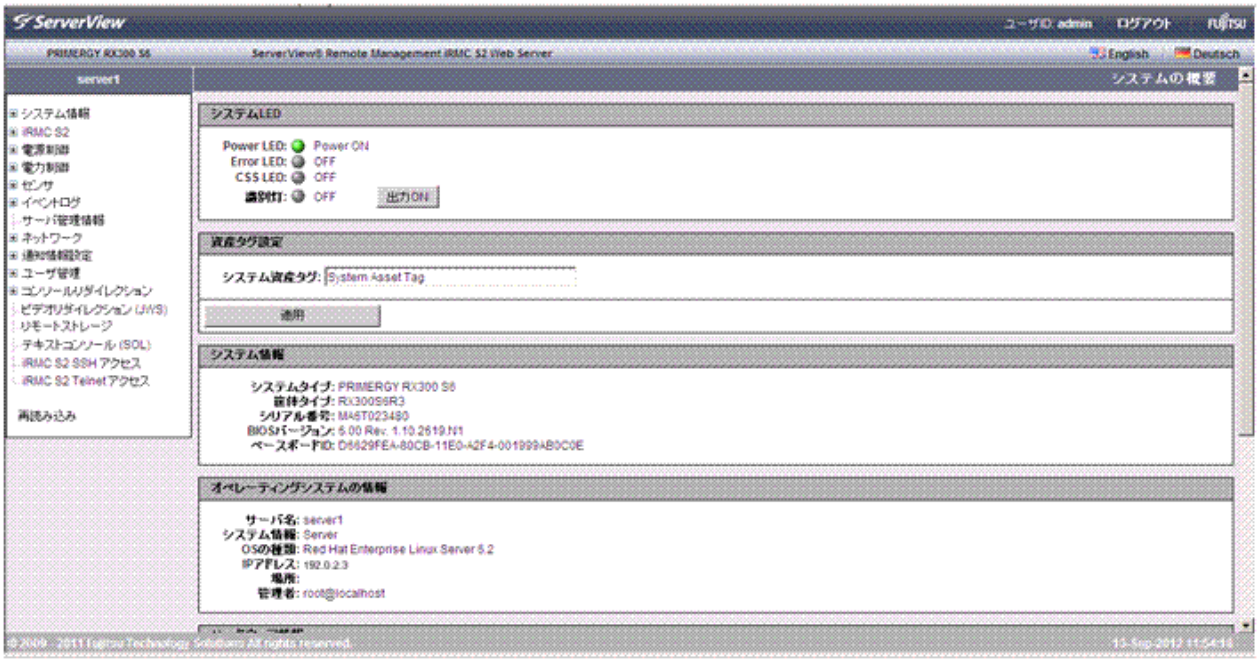
iRMCの電源制御機能を使って電源を投入する手順は以下のとおりです。

1. 管理端末でWebブラウザを起動します。
2. Webブラウザのアドレスバーに、“2.1.1 IPアドレスの準備”で用意したIPアドレス(“2.2.4 管理ネットワーク設定”で[サーバユニットのiRMC IP1]に設定したIPアドレス(注1))を利用したURLを入力します。

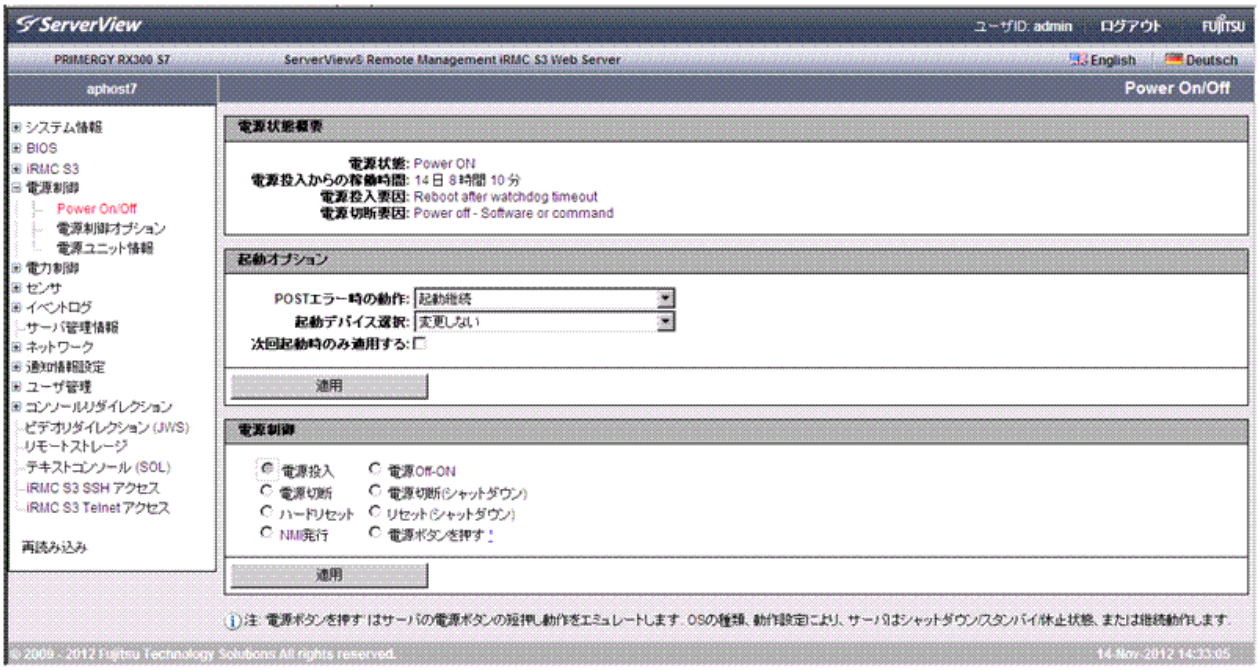
   ```
   http://サーバユニットのiRMC IP1/
   ```

   注1) [サーバユニットのiRMC IP2]を指定して電源を投入することも可能です。

   認証画面が表示されますので、ユーザー名:「admin」、パスワード(「admin」または “2.1.5 故障監視のための設定”の手順に従って変更したパスワード)でアクセスしてください。
3. 認証が完了すると以下の画面が表示されます。
   画面が英語で表示されている場合、画面右上の[日本語]リンクをクリックしてください。



4. 左画面のナビゲーションエリアのメニューで[電源制御]の[Power On/Off]を選択します。以下の画面が表示されます。



5. [電源制御]の画面から「電源投入」を選択し、[適用]ボタンをクリックします。
6. 画面右上の[ログアウト]リンクをクリックして、ログアウトします。

E.5.2 電源状態の確認

iRMCの電源制御機能を使って、電源状態を確認する手順は以下のとおりです。

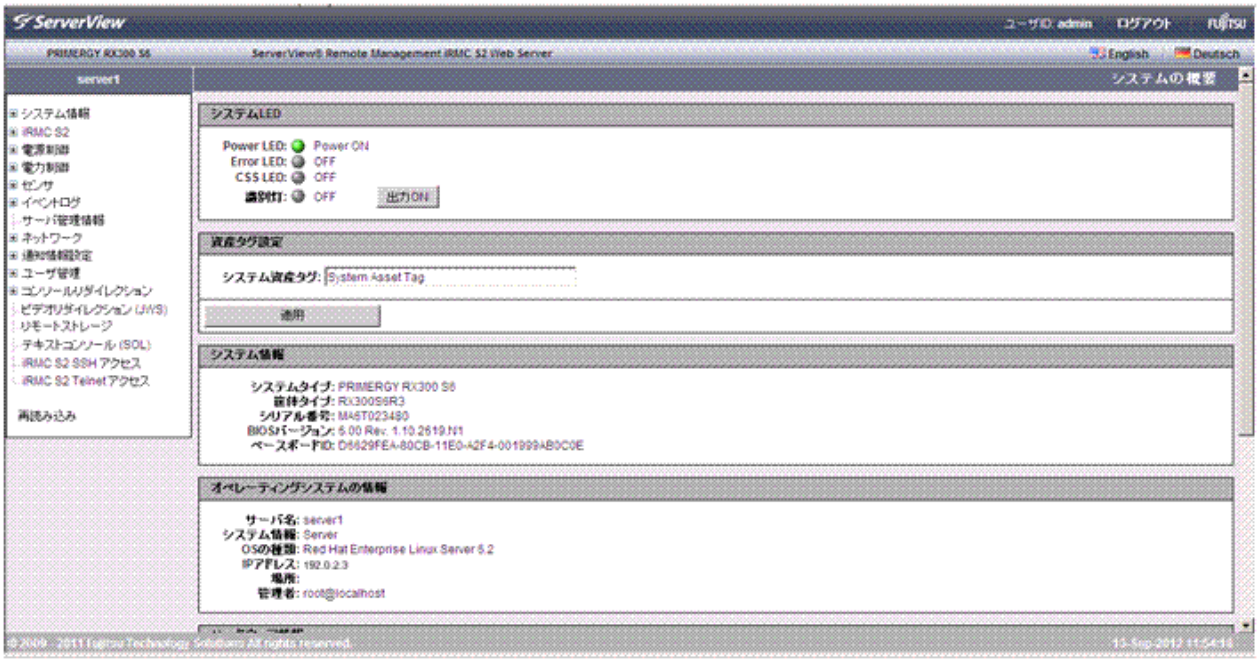
1. 管理端末でWebブラウザを起動します。
2. Webブラウザのアドレスバーに、“2.1.1 IPアドレスの準備”で用意したIPアドレス(“2.2.4 管理ネットワーク設定”で[サーバユニットのiRMC IP1]に設定したIPアドレス(注1))を利用したURLを入力します。

```
http://サーバユニットのiRMC IP1/
```

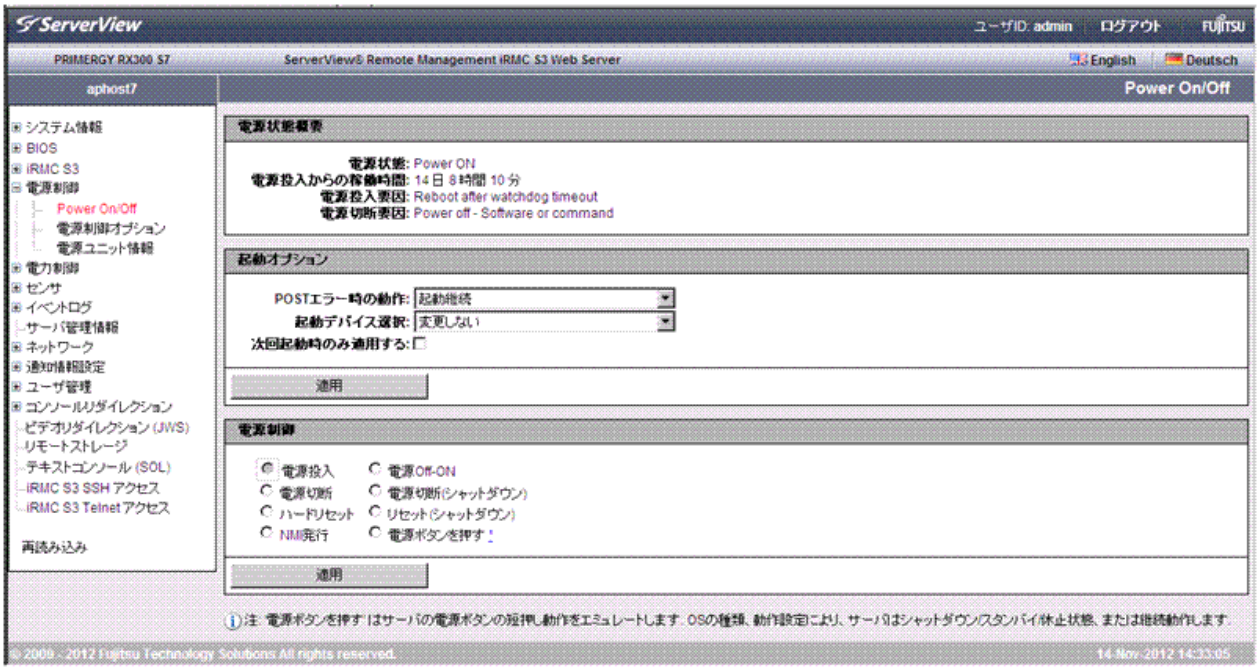
注1) [サーバユニットのiRMC IP2]を指定して電源を投入することも可能です。

認証画面が表示されますので、ユーザー名:「admin」、パスワード(「admin」または “2.1.5 故障監視のための設定”の手順に従って変更したパスワード)でアクセスしてください。

3. 認証が完了すると以下の画面が表示されます。
   画面が英語で表示されている場合、画面右上の[日本語]リンクをクリックしてください。



4. 左画面のナビゲーションエリアのメニューで[電源制御]の[Power On/Off]を選択します。以下の画面が表示されます。



5. [電源制御]の画面から[電源状態概要]を確認します。

付録F　Systemwalker Centric Managerの設定と運用

ここでは、Systemwalker Centric Managerをご利用のお客様がSystemwalker Centric ManagerでHA Database Readyの運用を管理する場合の基本的な設定と運用方法を説明します。

以降の手順は、HA Database Readyと連携する運用管理サーバに対して行います。
運用管理サーバまたは運用管理サーバに接続する運用管理クライアント上でSystemwalkerコンソールを起動して実施してください。

参照

- HA Database Readyにインストールされ ているSystemwalker Centric Manager(業務サーバ)のバージョンについては、“1.1.3 基本スペック”を参照してください。
- 接続可能な運用管理サーバのバージョンについては、“Systemwalker Centric Manager 解説書”の“運用管理サーバと部門管理サーバ/業務サーバ/クライアントの組み合わせ”を参照してください。

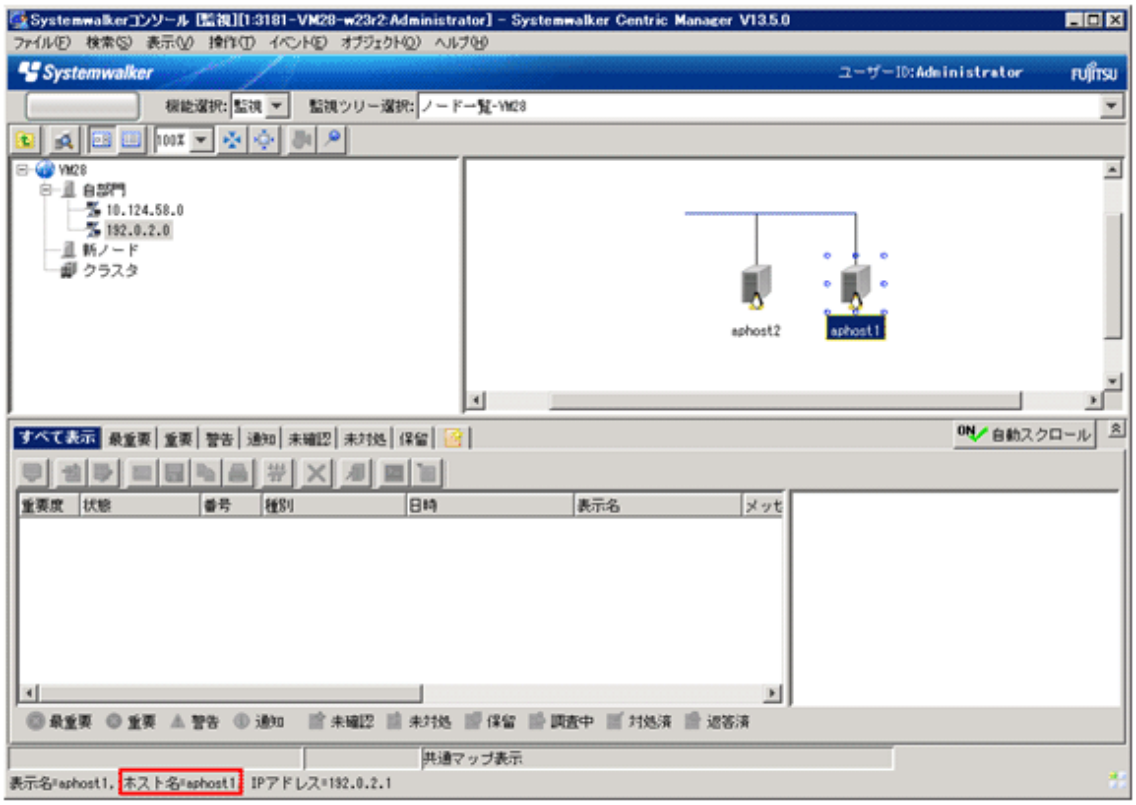
F.1　運用準備

1. 操作メニューへの登録
   操作メニューにAppliance Managerへのログイン用のメニューを登録します。Systemwalkerコンソールに登録されたHA Database Readyの2台のサーバに対して、以下のコマンドを実行してください。コマンドの詳細は、“Systemwalker Centric Manager リファレンスマニュアル”を参照してください。

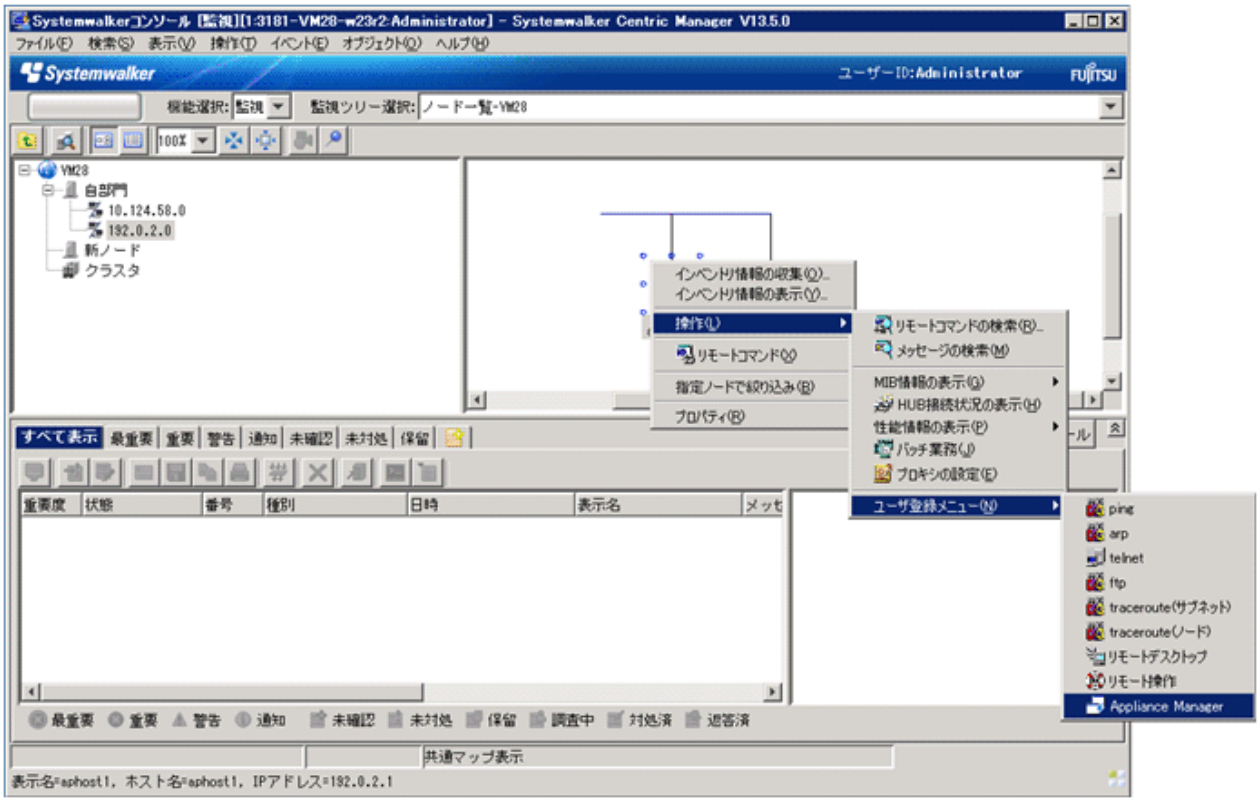
```
# mpaplreg -a -m "Appliance Manager" -p ホスト名(注) -c "https://%IP/appmgr" -w
```

注意

ホスト名は、Systemwalkerコンソールに登録されたHA Database Readyのサーバをクリックした時に左下に表示されるものを入力してください。ただし、ここで「ホスト名」に表示されるのは、“E.1 運用監視”で設定した[運用管理サーバで表示するホスト名]です。HA Database Readyのホスト名とは異なる場合があります。



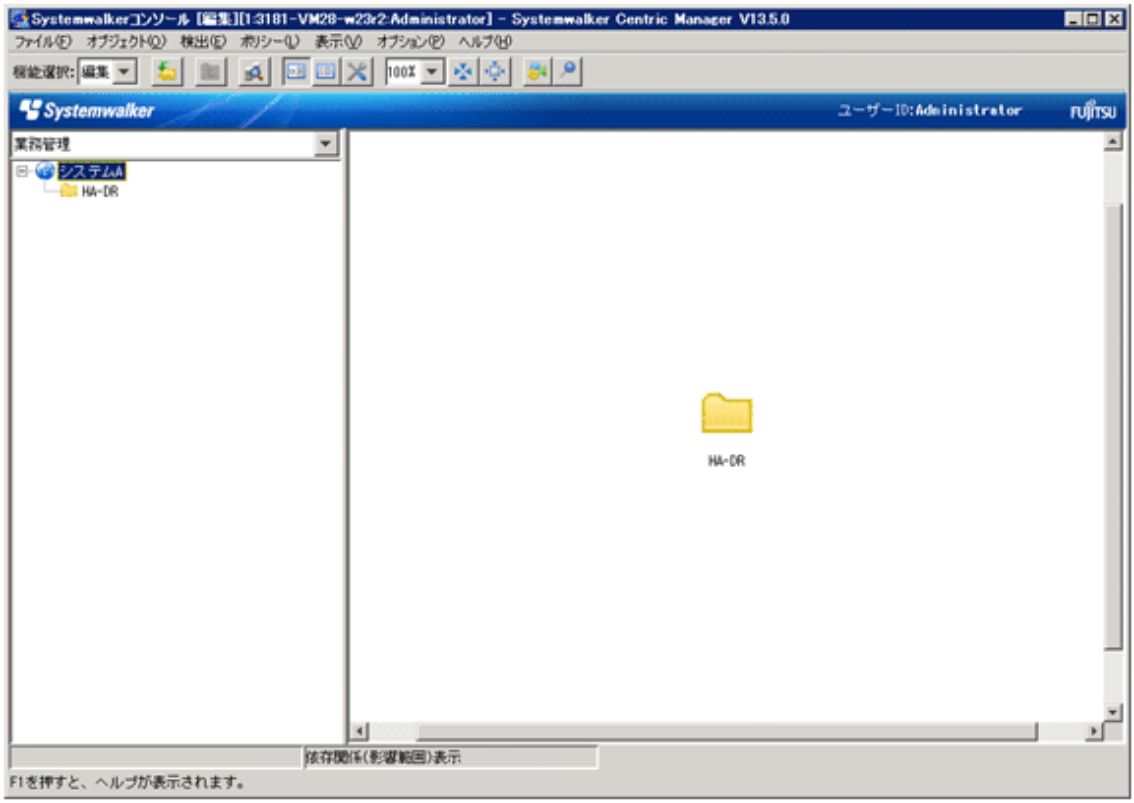
Systemwalkerコンソールを再起動した後、HA Database Readyのサーバを右クリックして[操作]-[ユーザ登録メニュー]-[Appliance Manager]とメニューが表示されれば、登録は正常に行われています。



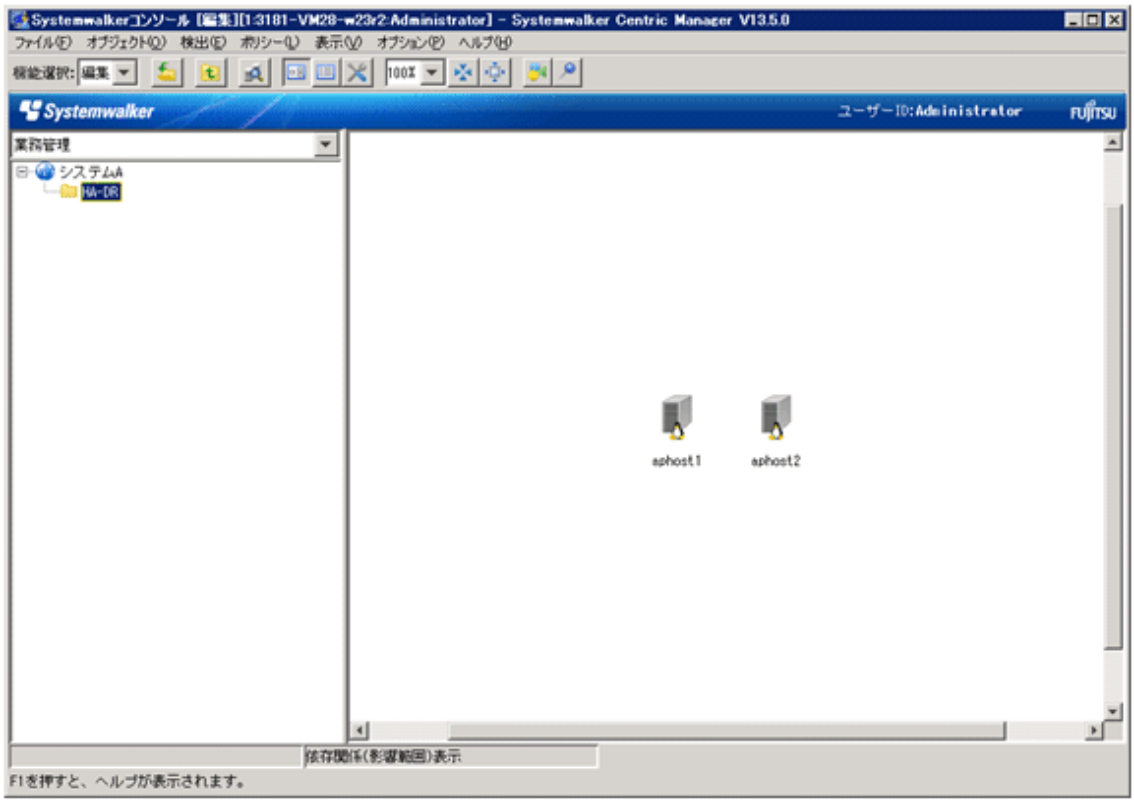
2. 業務管理ツリーへの登録

以下の手順で業務管理ツリーにHA Database Readyを登録します。業務ツリーの新規作成手順は“Systemwalker Centric Manager 使用手引書 監視機能編”を参照してください。システムAという業務ツリーにHA Database Readyを登録する手順を以下に示します。

a. HA Database Readyを表す業務（フォルダ）を作成します。ここではHA-DRという名前で作成したとします。



b. 手順a.で作成した業務の配下に、HA Database Readyを構成する2台のサーバを追加します。
以下は、HA-DRの配下にaphost1、aphost2というサーバを追加した場合の画面例です。

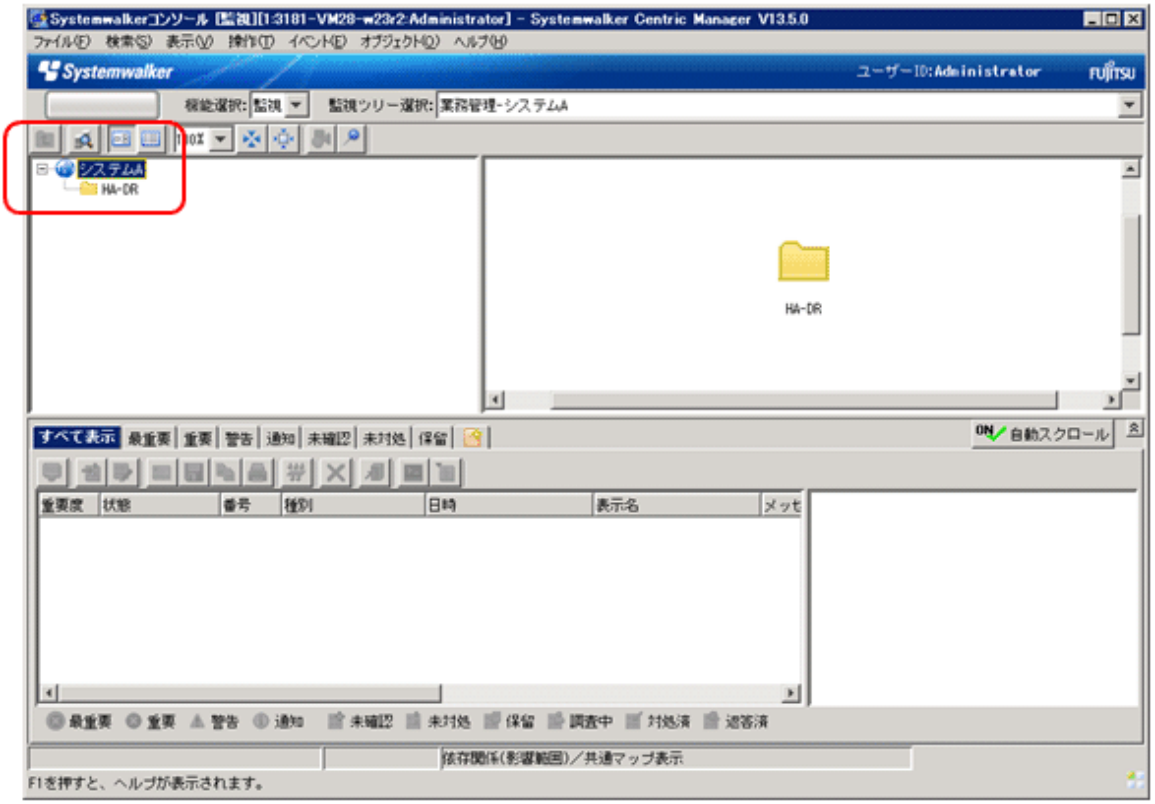


3. 他社の運用管理製品でHA Database Readyを管理する場合、Systemwalker Centric Managerの運用管理サーバから他社の運用管理製品へSNMPトラップを通知します。

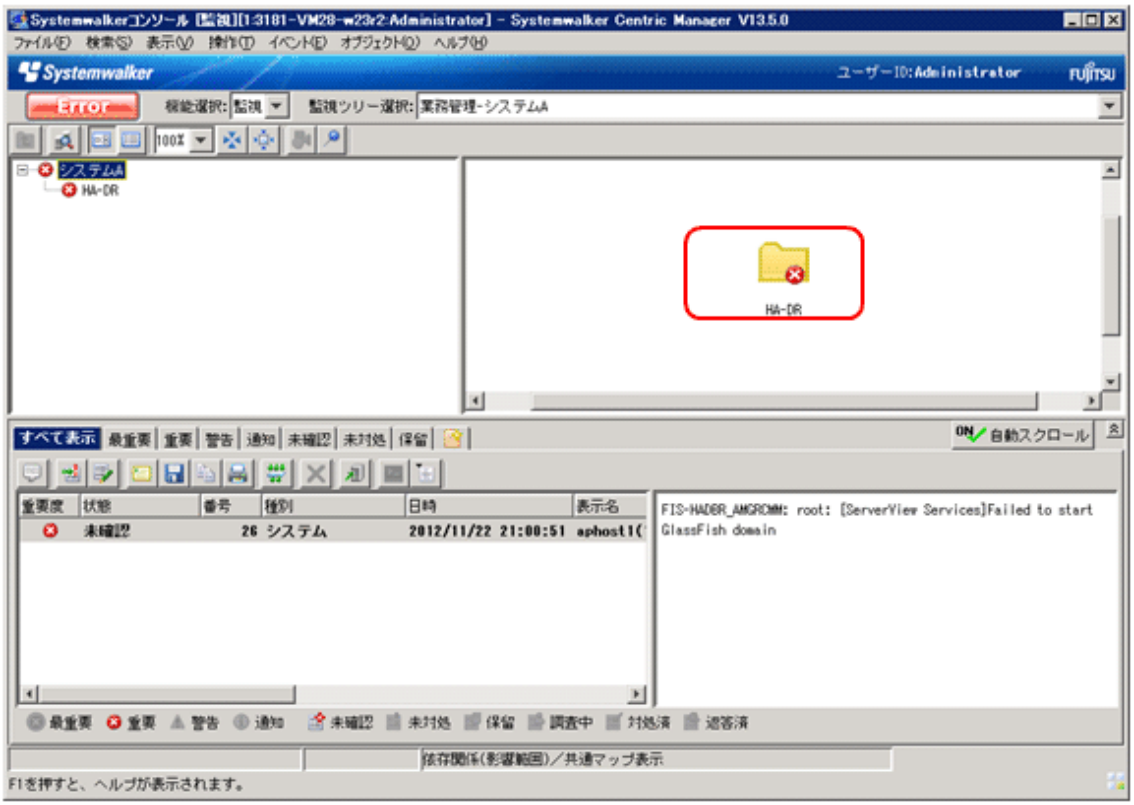
SNMPトラップを通知する方法については、“Systemwalker Centric Manager 使用手引書 監視機能編”の“SNMPトラップを発行する”を参照してください。

F.2　運用開始

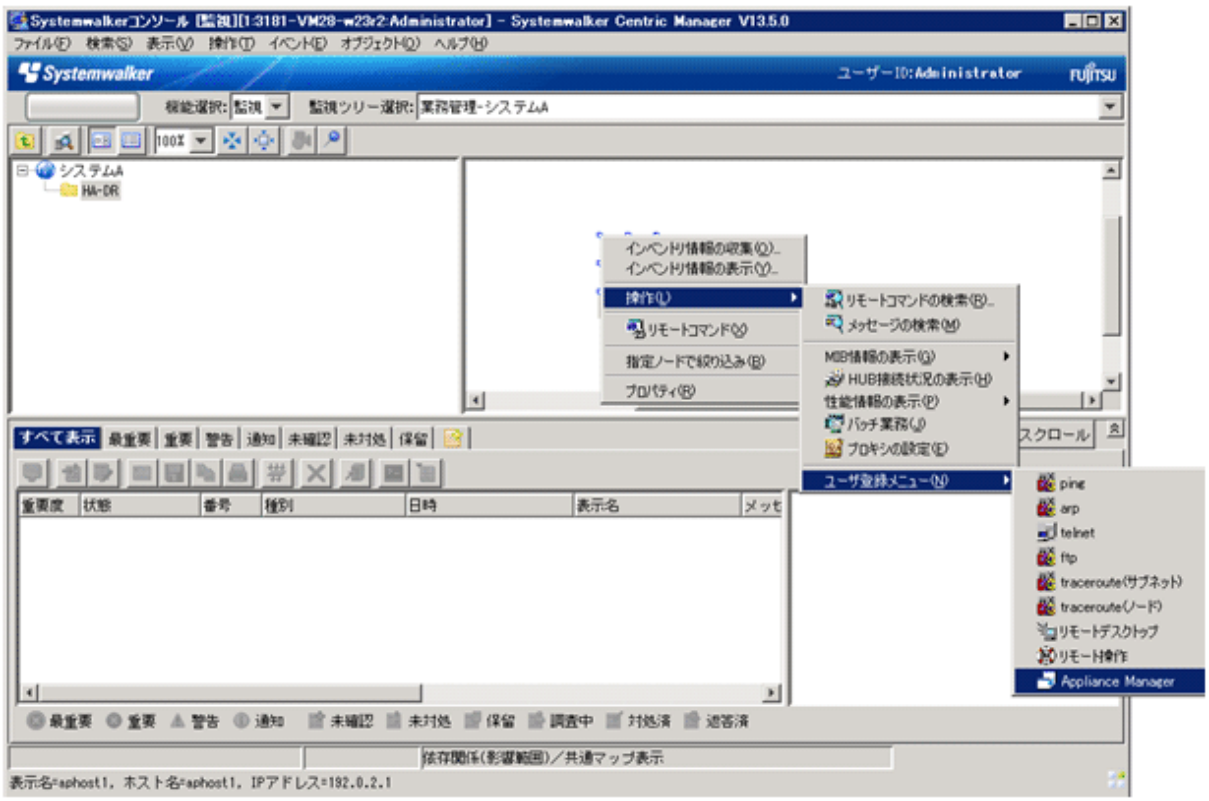
HA Database ReadyをSystemwalkerコンソールで監視するには、以下のように業務管理ツリーのシステムAを選択した状態にしておきます。



HA Database Readyで異常が発生した場合、以下のようにHA-DR（HA Database Readyを表す業務）に×印が表示されます。この×印で、異常を判断してください。



リカバリーなどのためにAppliance Managerへのログインが必要な場合、以下のようにaphost1またはaphost2を右クリックしてAppliance Manager（登録した操作メニュー）を選択することで、Appliance Managerにアクセスすることができます。



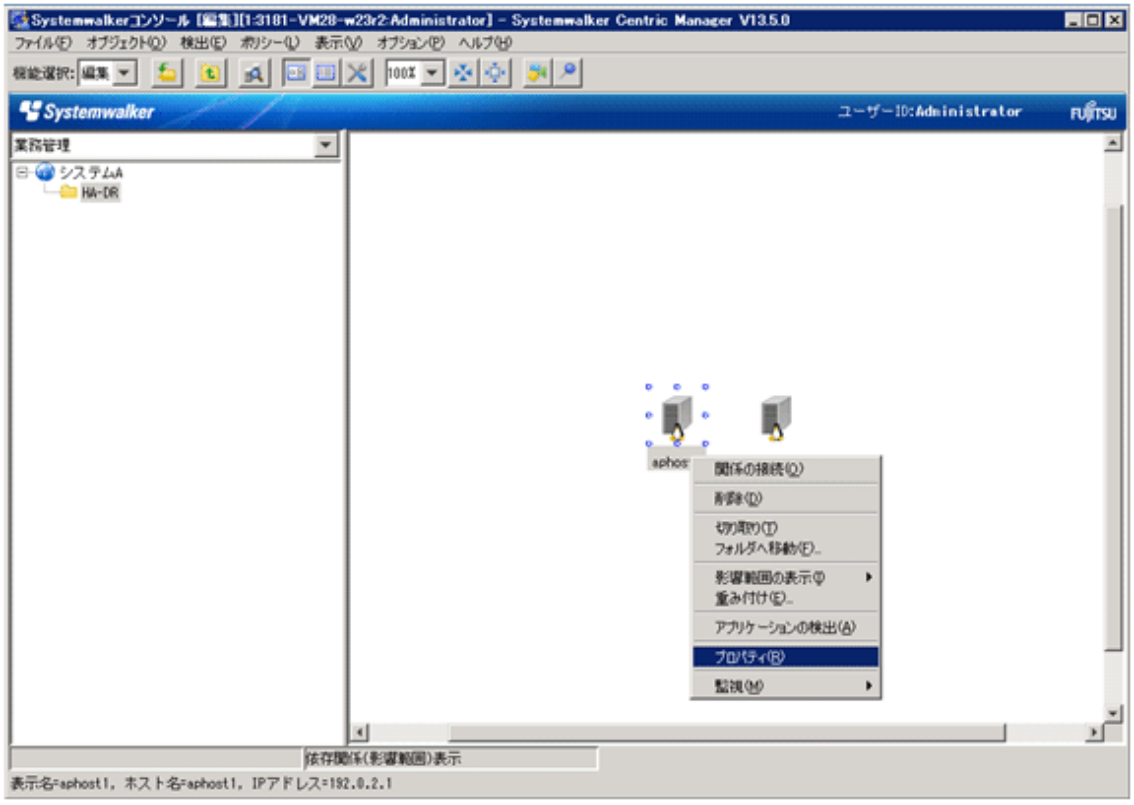
F.3　運用時の注意

運用時の注意事項について説明します。

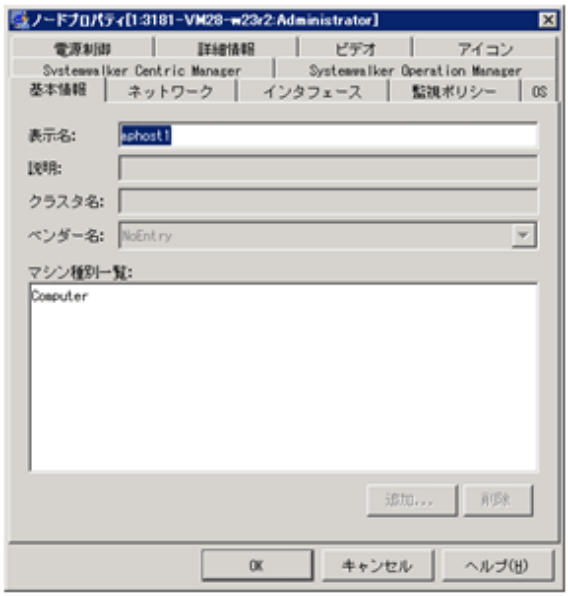
F.3.1　Systemwalkerコンソールでの表示名について

Appliance Managerで設定する[運用管理サーバで表示するホスト名]は、2回目以降の変更では運用管理サーバ上での表示が更新されません。[運用管理サーバで表示するホスト名]を変更した後に運用管理サーバ上の表示名も変更する場合、以下の手順にて実施してください。

1. Systemwalkerコンソールの編集モードで、表示名を変更したいサーバを右クリックし、[プロパティ]を選択します。



2.「表示名」を編集し、OKをクリックします。



F.3.2 HA Database Ready内のCentric Manager(業務サーバ)の正常起動確認について

HA Database Ready内のSystemwalker Centric Manager(業務サーバ)が正常に稼働していることを確認するには、Systemwalker Centric ManagerのSystemwalkerセルフチェック機能や、ノードの稼働状況監視の機能を利用してください。Systemwalkerセルフチェック機能については“Systemwalker Centric Manager API・スクリプトガイド”、ノードの稼働状況監視の機能については“Systemwalker Centric Manager 使用手引書 監視機能編”をそれぞれ参照してください。

F.4 使用制約

HA Database Readyとの連携時に使用できないSystemwalker Centric Managerの機能、および実施できない操作を示します。

運用管理の大分類	運用管理の小分類	Systemwalkerが提供する機能	使用可否	備考
構成の管理	ネットワークの構成情報の管理	ノードの検出	△	(注1)
		アプリケーションの検出	×	HA Database Readyでは、ソフトウェアの異常をサーバの異常として監視しているため不要。
	システムの構成情報の管理	インベントリ管理	×	
	コンソール	Systemwalkerコンソール	○	
		Systemwalker Webコンソール	○	
		Systemwalker Webコンソール(モバイル版)	○	
資源の配付	資源配付	資源配付	×	
		ロードバランサ制御配付	×	
ネットワーク/システムの監視	稼働監視	稼働状態の監視	△	(注1)
		仮想ノードの検出・監視	×	
	障害監視	トラップの監視	×	
		MIBしきい値監視	×	
		システムのイベント監視	△	Appliance Managerのメッセージウィンドウに通知されるイベントだけ監視可能。
	ネットワーク性能監視	性能異常の監視	×	
		性能情報の表示	×	
	サーバ性能監視	性能異常の監視	○	
		性能情報の表示	○	
	DHCP監視	DHCPクライアント監視	×	

運用管理の大分類	運用管理の小分類	Systemwalkerが提供する機能	使用可否	備考
	イベントコリレーション		△	HA Database Ready上での実現は不可。運用管理サーバ上での実現は可能(注2)。
	メッセージ変換		△	HA Database Ready上での実現は不可。運用管理サーバ上での実現は可能(注2)。
	イベント抑止		△	HA Database Ready上での実現は不可。運用管理サーバ上での実現は可能(注2)。
	監視抑止		○	
アプリケーションの監視	稼働監視	アプリケーションの稼働状態の表示	×	HA Database Readyでは、ソフトウェアの異常をサーバの異常として監視しているため不要。
		アプリケーションの稼働状態の監視	×	HA Database Readyでは、ソフトウェアの異常をサーバの異常として監視しているため不要。
	障害監視	アプリケーションのイベント監視	×	HA Database Readyでは、ソフトウェアの異常をサーバの異常として監視しているため不要。
	性能監視	性能異常の監視	×	HA Database Readyでは、ソフトウェアの異常をサーバの異常として監視しているため不要。
		性能情報の表示	×	HA Database Readyでは、ソフトウェアの異常をサーバの異常として監視しているため不要。
ソフトウェア修正管理			×	
ポリシー	ポリシーの配付		△	イベント監視のポリシーは編集不可(注2)。
	ポリシーの参照		△	
	ポリシーの移出		△	
Systemwalker自身の監視	イベントトレース	イベントトレース	×	
	プロセス監視	Systemwalkerのプロセス監視	△	HA Database Ready上でのコマンドによる状態表示は不可。
	ダウン監視	Systemwalkerセルフチェック	○	
	スローダウン監視	イベントのスローダウン監視	○	
	IPC資源の一元管理		△	HA Database Ready上でのコマンドによる状態表示は不可。
障害の復旧	リモートからの操作	リモート操作	×	
		リモートコマンド	×	
	リモートからの電源投入・切断	サーバの電源投入・切断	○	
		クライアントの電源投入・切断	×	
		(運用管理クライアントから運用管理サーバを経		

運用管理の大分類	運用管理の小分類	Systemwalkerが提供する機能	使用可否	備考
		由して操作できます。)		
	障害対処の自動化	自動アクション	△	HA Database Readyでの実現は不可。運用管理サーバ上での実現は可能(注2)。
返答メッセージ			×	
評価	監査ログ分析		×	
	ネットワークの評価	レポーティング	○	
	システムの評価	レポーティング	○	
セキュリティ	サーバアクセス制御		×	
	サーバ操作制御		×	
	コンソール操作制御		○	
	操作ログ出力		×	
	監査ログ出力		×	
	監査ログ管理		×	
	監査ログ分析		×	
	稼働状況の監視	Webサービスの稼働監視	×	
共通(さまざまなシステムでの利用)	高信頼システムの管理	クラスタ構成の管理	×	
		クラスタサービスの稼働監視		
		業務サーバのクラスタ化	×	
		LAN二重化環境の監視	×	
	管理サーバの高信頼化	管理サーバのクラスタ化	○	
		(EE版の運用管理サーバ、部門管理サーバで使用できます。)		
		運用管理サーバ二重化	○	
	大規模システム	全体監視	○	
		(EE版の運用管理サーバで使用できます。)		
Systemwalkerスクリプト			×	
トラブルシューティング	調査資料の採取	保守情報収集ツール	×	

○ : 使用可能
△ : 使用できる機能に制限あり
× : 使用不可能

注1) SNMPエージェントを使用しない以下の機能が使えます。
・ノード検出（IP/ホスト名だけ）
・稼働状態の監視（起動/停止だけ）
各機能の詳細については、“Systemwalker Centric Manager使用手引書 監視機能編”を参照してください。
注2)イベント監視の監視条件と動作環境のポリシーは「ローカル設定を利用する」に固定した状態にします。上記以外を設定するとポリシー配付に失敗します。

付録G　サーバへのログイン方法

HA Database Readyでは、Appliance Managerの操作でシステムの設定や、運用操作を行いますが、一部の設定や運用操作でサーバにログインする必要が生じる場合があります。

サーバへは、スーパーユーザーでログインします。

以下の情報を参照し、管理端末から端末エミュレータソフトウェアを使用して、接続してください。

接続先のサーバの情報

項目	値
IPアドレス	管理用のIPアドレス (“2.2.4 管理ネットワーク設定”で[サーバユニットIP1]、[サーバユニットIP2]に指定したIPアドレス)
接続プロトコル	SSH2プロトコル
接続時のユーザーID	root
パスワード	rootのパスワード(注)
ログイン時のロケール	ja_JP.UTF-8
作業ディレクトリ	/home

注) “2.1.4 サーバのパスワード設定”の手順2で変更した新しいパスワードです。

注意

- お客様が使用可能なディレクトリがあらかじめ決められています。以下に示すディレクトリまたはファイル以外の削除または更新をしないでください。
  - 接続先のサーバの情報で示した“作業ディレクトリ”配下
  - “付録D 運用の詳細設定”および“付録E 運用管理サーバとの連携”で使用しているディレクトリおよびファイル
- サーバで、お客様が作成したアプリケーションは実行しないでください。
  HA Database Readyは、データベースが高性能で動作する最適値にチューニングされています。ユーザー・アプリケーションの実行により、HA Database ReadyのCPUリソース、メモリリソースが消費されると、データベースのパフォーマンスに悪影響が出ます。
- 端末エミュレータソフトウェア上に、以下のメッセージが表示される場合があります。これはCPUに対する無効な割込が発生したことを意味しますが、HA Database Readyの運用に影響はありません。

```
kernel: do_IRQ: X.Y No irq handler for vector (irq -1)
```

  X: CPU番号が表示されます。
  Y: ベクタ番号が表示されます。

付録H　購入時の状態

HA Database Readyを構成する機器の購入時の状態を説明します。

H.1　IPアドレス

HA Database Readyを構成する機器の購入時のIPアドレスを説明します。

サーバ

使用しているネットワーク		IPアドレス	
管理ネットワーク	構成機器用アドレス	192.168.1.10	192.168.1.11
	iRMC用アドレス	192.168.1.20	192.168.1.21
業務ネットワーク		172.20.10.10	172.20.10.11

ストレージ

使用しているネットワーク		IPアドレス
管理ネットワーク	構成機器用アドレス	192.168.1.220 192.168.1.230

外部接続スイッチ

使用しているネットワーク		IPアドレス
管理ネットワーク	構成機器用アドレス	192.168.1.100 192.168.1.101

内部ネットワーク

使用しているネットワーク	IPアドレス
内部ネットワーク	192.168.2.* 192.168.3.* 192.168.4.*

参考

HA Database Readyの購入時のサブネットマスクは“255.255.255.0”です。

H.2　ホスト名

サーバ

ラベル名	ホスト名
ServerUnit#1	aphost1
ServerUnit#2	aphost2

ServerView Operations Managerを利用するには、管理端末でServerUnit#1、ServerUnit#2の名前解決ができるよう設定されている必要があります("3.1 管理端末の設定"参照)。
ホスト名を変更したい場合は、“D.7 ホスト名の変更”を参照してください。

H.3　時刻設定

サーバ

サーバ(ServerUnit#1およびServerUnit#2)のタイムゾーンは、「アジア/東京」に設定されています。また、システムクロックはUTCを使用しています。

付録I　デザインシート

HA Database Readyのセットアップで必要な項目です。お客様の設定値を記入して、セットアップ時に使用してください。

表I.1 IPアドレス

項目			説明で使用する値	お客様の設定値	備考
業務ネットワーク	IPv4	IPv4アドレスを指定する	□IPv4アドレスを指定する	□IPv4アドレスを指定する	・業務ネットワーク上の同一のサブネットに存在するIPv4形式またはIPv6形式のIPアドレスが必要です。IPv4とIPv6の両方の形式のIPアドレスを同時に指定可能です。
		IP1	172.20.10.10	(1)	
		IP2	172.20.10.11	(2)	
		Netmask	255.255.255.0	(3)	
		Gateway	172.20.10.1	(4)	
	IPv6	IPv6アドレスを指定する	□IPv6アドレスを指定する	□IPv6アドレスを指定する	
		IP1	-	(5)	
		IP2	-	(6)	
		Prefix Size	-	(7)	
		Gateway	-	(8)	
内部ネットワーク (第3オクテットが連続している3つのサブネットを使用します)			192.168.2.0～255	(9)	・第3オクテットが連続している3つのサブネットを自動的に使用します 例)192.168.2.0～255を指定すると、192.168.2.0～255、192.168.3.0～255、192.168.4.0～255が内部ネットワークに使用されます。
管理ネットワーク	サーバユニット	IP1 (管理用のIPアドレス)	192.168.1.10	(10)	・管理ネットワーク上の同一のサブネットに存在するIPv4形式のIPアドレスが必要です。 ・導入時に、サーバユニットのIP1を設定し、[自動採番する]ボタンを押下するとその他のIPアドレスが連番で自動設定されるため、連番で設定することを推奨します。
		IP2 (管理用のIPアドレス)	192.168.1.11	(11)	
		iRMC IP1 (iRMCのIPアドレス)	192.168.1.12	(12)	
		iRMC IP2(iRMCのIPアドレス)	192.168.1.13	(13)	
	ストレージユニット	IP1	192.168.1.14	(14)	
		IP2	192.168.1.15	(15)	
	外部接続スイッチ	IP1	192.168.1.16	(16)	
		IP2	192.168.1.17	(17)	
	Netmask		255.255.255.0	(18)	

表I.2 データベース

項目	初期値	お客様の設定値	備考
データベースインターフェース	Open SQL		
データベースの文字コード	UTF8		

項目	初期値	お客様の設定値	備考
ポート番号 (注)	26500		

注) ポート番号に指定可能な値は、5432および26500～26999です。初期値は以下です。
・Open SQLインターフェースの場合 ：26500
・Native SQLインターフェースの場合：26551

表I.3 ユーザーID

項目	ID/Password	購入時の値	お客様の設定値	備考
サーバ設定	ユーザーID	root	(変更不可)	接続プロトコルssh2、ログイン時のロケールja_JP.UTF-8
	パスワード (注1)	rootroot		
iRMC(故障監視設定)	ユーザー名	admin	(変更不可)	
	パスワード (注2)	admin		
Appliance Manager設定	ユーザーID (注3)	administrator		Appliance Managerとデータベースの管理用です。
	パスワード (注4)	administrator		

注1) 6文字以上。
注2) 1～20文字(8文字以上を推奨します)。半角英数字と記号が指定可能。ただし、以下の記号は指定できません。
> < " / ¥ = ! ? ; , &
注3) 1～18文字。先頭が半角英字、2文字目以降は半角英数字が使用可能。
注4) 8～16文字。半角英数字、アンダースコア、ピリオドが使用可能。

付録J　トラブルシューティング

本章では、HA Database Readyのトラブルへの対処方法について説明します。

J.1　セットアップ中にトラブルが発生した場合の対処方法

HA Database Readyのセットアップ中にトラブルが発生した場合の対処方法について説明します。

“クイックスタートガイド”または“利用ガイド”に従ってセットアップを行ったが、セットアップ作業が正しく完了しない、セットアップ中に“クイックスタートガイド”または“利用ガイド”の状態と異なる、などのトラブルが発生した場合、HA Database Readyの状態を確認し、“J.2 問合せ時に必要な情報”に従って弊社保守員に連絡してください。

ポイント

“クイックスタートガイド”は、印刷物として製品添付されています。

または、HA Database Ready製品のホームページからも参照できます。

注意

以下の各STEPは“クイックスタートガイド”の流れに対応しています。

J.1.1　STEP2 セットアップ

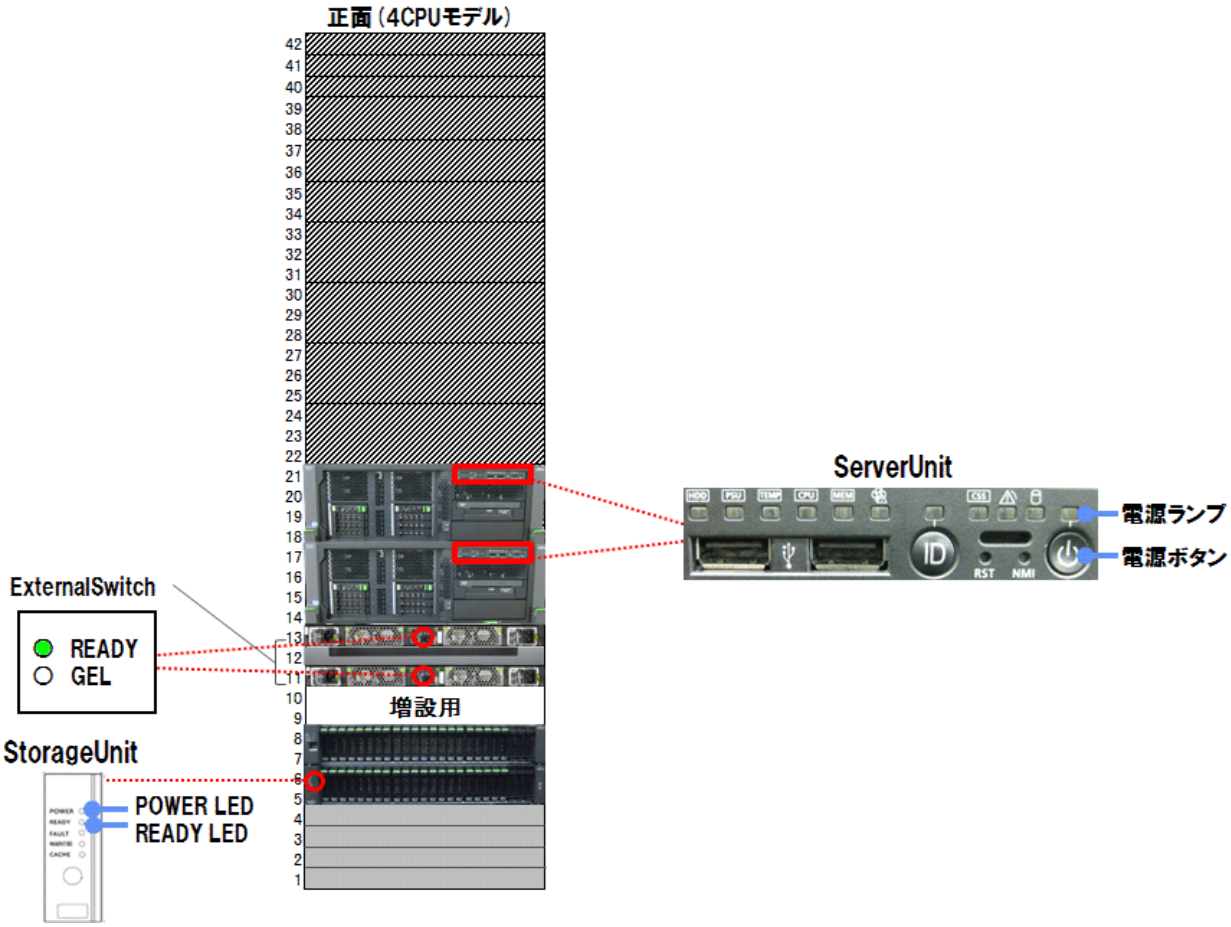
HA Database Readyのセットアップ時の確認事項です。

事象	詳細事象
HA Database Readyの構成装置の電源ランプ、またはREADYランプが点灯しない	・ ServerUnitの電源ランプがオレンジ色に点灯しない場合 ・ ExternalSwitch のREADYランプが緑色に点灯しない場合
HA Database Readyの構成装置のLEDが“クイックスタートガイド”、または“利用ガイド”の状態と異なっている	・ ServerUnitの保守ランプがオレンジ色に点灯・点滅している場合 ・ StorageUnitのFAULT LEDがオレンジ色に点灯・点滅している場合 ・ ExternalSwitchのGELランプがオレンジ色に点灯している場合
電源投入操作実行後、約15分経過してHA Database Readyの構成装置のLEDが“クイックスタートガイド”または“利用ガイド”の状態と異なっている	・ ServerUnitの保守ランプがオレンジ色に点灯・点滅している場合 ・ StorageUnitのFAULT LEDがオレンジ色に点灯・点滅している場合 ・ ExternalSwitchのGELランプがオレンジ色に点灯している場合 ・ ServerUnit#1の電源ランプが緑色に点灯しない場合 ・ ServerUnit#2の電源ランプが緑色に点灯しない場合

事象	詳細事象
	・ StorageUnitのPOWER LEDが緑色に点灯しない場合 ・ StorageUnitのREADY LEDが緑色に点灯しない場合
ログインできない	・ ServerUnitのOSへログインができない場合 ・ ServerUnitのiRMCへログインができない場合 ・ Appliance Managerへログインができない場合 ・ セットアップ中にエラーが発生した場合

HA Database Readyの構成装置の電源ランプ、またはREADYランプが点灯しない

図J.1 HA Database Ready 各構成装置の電源ランプ



ServerUnitの電源ランプがオレンジ色に点灯しない場合

ー ServerUnitの電源コードが抜けていませんか。
ServerUnitの電源コードを挿しなおしてください。

ー 現在停電中ではありませんか。
停電状態から復旧を行ってください。

ExternalSwitch のREADYランプが緑色に点灯しない場合

- ExternalSwitchの電源コードが抜けていませんか。
  ExternalSwitchの電源コードを挿しなおしてください。

- 現在停電中ではありませんか。
  停電状態から復旧を行ってください。

HA Database Readyの構成装置のLEDが“クイックスタートガイド”、または“利用ガイド”の状態と異なっている

ServerUnitの保守ランプがオレンジ色に点灯・点滅している場合

- ServerUnitに異常・故障が発生しています。
  弊社保守員へ連絡してください。

図J.2 ServerUnit前面LED

StorageUnitのFAULT LEDがオレンジ色に点灯・点滅している場合

- StorageUnitに異常が発生しています。
  弊社保守員へ連絡してください。

図J.3 StorageUnit前面LED

ExternalSwitchのGELランプがオレンジ色に点灯している場合

- ExternalSwitchに異常が発生しています。
  弊社保守員へ連絡してください。

図J.4 ExternalSwitch LED

電源投入操作実行後、約15分経過してHA Database Readyの構成装置のLEDが“クイックスタートガイド”または“利用ガイド”の状態と異なっている

ServerUnitの保守ランプがオレンジ色に点灯・点滅している場合

- STEP2を参照し、状態を確認後、弊社保守員へ連絡してください。

StorageUnitのFAULT LEDがオレンジ色に点灯・点滅している場合

- STEP2を参照し、状態を確認後、弊社保守員へ連絡してください。

ExternalSwitchのGELランプがオレンジ色に点灯している場合

- STEP2を参照し、状態を確認後、弊社保守員へ連絡してください。

ServerUnit#1の電源ランプが緑色に点灯しない場合

- ServerUnit#1の電源コードが抜けていませんか。
  ServerUnit#1の電源コードを挿しなおし、電源ボタンを押して約15分間お待ちください。

- 現在停電中ではありませんか。
  停電状態から復旧後、ServerUnit#1の電源ボタンを押して約15分間お待ちください。

ServerUnit#2の電源ランプが緑色に点灯しない場合

- ExternalSwitch#1のport3、port6、ServerUnit#1のLOM1、ServerUnit#2のiRMCに接続されているツイストペアケーブルは抜けていませんか(各接続ポートの実装位置については“設置ガイド”の“構成装置の背面図”および“ケーブル接続一覧”を参照してください)。
  ツイストペアケーブルを挿しなおし、ServerUnit#2の電源ボタンを押して約15分間お待ちください。

- ServerUnit#2の電源コードが抜けていませんか。
  ServerUnit#2の電源コードを挿しなおし、ServerUnit#2の電源ボタンを押して約15分間お待ちください。

- 現在停電中ではありませんか。
  停電状態から復旧後、ServerUnit#2の電源ボタンを押し、約15分間お待ちください。

StorageUnitのPOWER LEDが緑色に点灯しない場合

- StorageUnitの電源コードが抜けていませんか。
  StorageUnitの電源コードを挿しなおしてください。接続後、ServerUnit#1の電源ランプが緑色に点灯している場合電源ボタンを押し、シャットダウンを行ってください。

同様の作業をServerUnit#2にも行ってください。
電源ランプがオレンジ色に点灯している場合は、電源ボタンを押す必要はありません。
シャットダウン後、再度、ServerUnit#1の電源ボタンを押して、電源投入を行ってください。

- ExternalSwitch#1のport2、port3、ServerUnit#1のLOM1、StorageUnitのCM0# MNTに接続されているツイストペアケーブルは抜けていませんか(各接続ポートの実装位置については“設置ガイド”の“構成装置の背面図” および“ケーブル接続一覧”を参照してください)。
  ツイストペアケーブルを挿しなおしてください。接続後、ServerUnit#1の電源ランプが緑色に点灯している場合電源ボタンを押し、シャットダウンを行ってください。
  同様の作業をServerUnit#2にも行ってください。
  電源ランプがオレンジ色に点灯している場合は、電源ボタンを押す必要はありません。
  シャットダウン後、再度、ServerUnit#1の電源ボタンを押して、電源投入を行ってください。

StorageUnitのREADY LEDが緑色に点灯しない場合

- StorageUnitに異常が発生しています。
  弊社保守員へ連絡してください。

ログインできない

ServerUnitのOSへログインができない場合

- セットアップ用PCのLANポート、ExternalSwitch#1のport1、port3、port4、ServerUnit#1のLOM1、ServerUnit#2のLOM1に接続されているツイストペアケーブルが抜けていませんか(各接続ポートの実装位置については“設置ガイド”の“構成装置の背面図” および“ケーブル接続一覧”を参照してください)。
  ツイストペアケーブルを挿しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- ServerUnit#1のIPアドレスは、[192.168.1.10]と入力されていますか。
  正しいIPアドレスを入力しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- ServerUnit#2のIPアドレスは、[192.168.1.11]と入力されていますか。
  正しいIPアドレスを入力しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- セットアップ用PCのIPアドレスは、[192.168.1.30]に設定されていますか。
  正しいIPアドレスを設定しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- サーバのパスワード変更時にユーザーIDは[root]、パスワードは[rootroot]と入力されていますか。
  正しいユーザーIDとパスワードを入力しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、ログインをしなおしてください。

ServerUnitのiRMCへログインができない場合

- セットアップ用PCのLANポート、ExternalSwitch#1のport1、port5、port6、ServerUnit#1のiRMC、ServerUnit#2のiRMCに接続されているツイストペアケーブルが抜けていませんか(各接続ポートの実装位置については“設置ガイド”の“構成装置の背面図” および“ケーブル接続一覧”を参照してください)。
  ツイストペアケーブルを挿しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- ServerUnit#1のiRMCのIPアドレスは、[192.168.1.20]と入力されていますか。
  正しいIPアドレスを入力しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- ServerUnit#2のiRMCのIPアドレスは、[192.168.1.21]と入力されていますか。
  正しいIPアドレスを入力しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- セットアップ用PCのIPアドレスは、[192.168.1.30]に設定されていますか。
  正しいIPアドレスを設定しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- 故障監視の設定時にユーザーIDとパスワードは[admin]と入力されていますか。
  正しいユーザーIDとパスワードを入力しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、ログインをしなおしてください。

Appliance Managerへログインができない場合

- セットアップ用PCのLANポート、ExternalSwitch#1のport1、port3、ServerUnit#1のLOM1に接続されているツイストペアケーブルが抜けていませんか(各接続ポートの実装位置については“設置ガイド”の“構成装置の背面図” および“ケーブル接続一覧”を参照してください)。
  ツイストペアケーブルを挿しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- セットアップ用PCのIPアドレスは、[192.168.1.30]に設定されていますか。
  正しいIPアドレスを設定しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- 入力したAppliance ManagerのURLは[http://192.168.1.10/appmgr]に設定されていますか。
  正しいURLを入力しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

- ユーザーIDとパスワードは[administrator]と入力されていますか。
  正しいユーザーIDとパスワードを入力しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、ログインをしなおしてください。

セットアップ中にエラーが発生した場合

- セットアップ中に内部エラーが発生しました。
  弊社保守員に連絡してください。

J.1.2 STEP3 動作確認

HA Database Readyの動作確認時の確認事項です。

まずSTEP2の確認を行ってください。異常がない場合、以下の確認を実施してください。

・ **Appliance Managerの画面参照ができない場合**

ー ExternalSwitch#1のport1、port3、ServerUnit#1のLOM1に接続されているツイストペアケーブルが抜けていませんか(各接続ポートの実装位置については“設置ガイド”の“構成装置の背面図” および“ケーブル接続一覧”を参照してください)。
ツイストペアケーブルを挿しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

ー 入力したAppliance ManagerのURLは間違っていませんか。
正しいURLを入力しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

ー 管理端末のIPアドレスが間違っていませんか。
正しいIPアドレスを設定しなおし、再度“クイックスタートガイド”または“利用ガイド”に従って、アクセスをしなおしてください。

J.2 問合せ時に必要な情報

トラブル発生時に弊社保守員へ連絡する場合は、以下の情報を準備して、保守サービスに応じた担当に連絡してください。

・ 故障装置の型名と製造号機
Appliance Managerの[製品情報]リンクをクリックすると、型名と製造号機が参照できます。操作方法は“[製品情報]”を参照してください。

・ トラブルの内容、お客様が行った対処とその結果

・ HA Database Ready構成装置(ServerUnit、StorageUnit、ExternalSwitch)

・ HA Database Readyのログ/ダンプ情報
(“3.6.3 調査資料の採取”を参照し、情報を採取してください。)

保守サービスについて

HA Database Readyの製品保証期間中は、保証書に記載された内容に従い、無償で修理を受けることができます。

無償修理を受ける場合は、必ず保証書を用意し、保証書に記載された「ハードウェアの故障/修理のご相談窓口」に連絡してください。

無償修理期間外の修理のご相談は、担当営業員または担当の弊社保守員に連絡してください。

J.3 使用上の留意事項

HA Database Readyの使用に関し、以下の留意事項があります。製品をご使用になる前にお読みください。

J.3.1 サーバユニットの留意事項

サーバユニットにはご使用にあたっての留意事項があります。以下サイトにて公開していますのでご使用になる前にお読みください。

```
http://jp.fujitsu.com/platform/server/primergy/manual/pdf/rx500s7/rx500s7-note.pdf
```

J.3.2 外部接続スイッチの留意事項

外部接続スイッチにはご使用にあたっての留意事項があります。以下サイトにて公開していますのでご使用になる前にお読みください。

http://jp.fujitsu.com/platform/server/primergy/manual/peri_blade.html#py-cfb101

上記サイトより“コンバージドファブリックスイッチ製品 ご使用上の留意・注意事項”を参照ください。

索　引

[A]

Appliance Manager..... 7,17,25
Appliance Managerへのログイン.....25
Appliance Managerへのログイン(セットアップ)..... 17

[B]

BIOSファームウェアの更新.....48

[D]

DMZ.....5

[F]

FIS-HADBR_AMGRCMEで始まるメッセージ..... 58
FIS-HADBR_AMGRDBで始まるメッセージ..... 52

[H]

HA Database Ready.....1
HA Database Readyとは..... 1
HA Database Readyの運用..... 10
HA Database Readyの概要..... 1
HA Database Readyの特長..... 7

[I]

ip6tables..... 5
iptables..... 5
IPアドレスの確認..... 64
IPアドレスの準備..... 12
iRMC.....4

[J]

JREのインストール..... 24

[N]

Native SQL.....7
NetVault Backup.....71
NTP.....4
NTPサーバ..... 11

[O]

Open SQL.....7

[P]

PCIe SSD..... 7

[S]

ServerViewコンソール.....29
SMTP..... 4
SMTPサーバ..... 10
Systemwalker Centric Managerの設定と運用.....98

[W]

Webブラウザの設定..... 24,61

[あ]

インターネット..... 5
インターネットを利用した接続形態..... 4
イントラネット..... 5
運用..... 24
運用監視.....4,26,88
運用管理サーバ..... 3
運用管理サーバとの連携..... 88
運用時の注意(運用管理サーバ).....104
運用準備(運用管理サーバ)..... 98
運用情報の通知メール.....93
運用中の容量追加..... 9
運用の詳細設定..... 64
運用変更.....35
オープン性.....7

[か]

外部ネットワークとの接続..... 22
外部バックアップ..... 10,71
外部バックアップの事前準備..... 72
外部バックアップ用のサーバ..... 4
外部バックアップを用いたリカバリー..... 77
鍵管理サーバ.....4,82
格納データの暗号化.....81
稼働状態.....26
簡単運用.....8
簡単導入.....7
管理端末.....3,25,109
管理端末の設定..... 24
管理ネットワーク..... 3,20
管理ネットワーク設定.....20
管理ネットワークの経路設定..... 25,69
管理用のユーザーID.....18
管理用のユーザーIDの設定.....18
管理用のユーザーIDのパスワード..... 35
管理用のユーザーIDのパスワード変更.....35
機器の準備.....12
基本スペック.....6
業務ネットワーク..... 3,19
業務ネットワーク、内部ネットワーク設定.....18
キーストアの格納場所.....82
警告・異常時の対処とリカバリー.....30
ゲートウェイ.....64,69
高性能..... 7
購入時のIPアドレス..... 110
故障監視のための設定.....15

[さ]

最新情報に更新ボタン.....28
サーバのパスワード設定..... 15
サーバのホスト名の変更..... 11
サーバへのログイン方法..... 109
時刻補正.....4,89
システム構成.....3
自動更新を有効にする.....28

シャットダウン..... 50
修正..... 36
修正削除..... 39
修正適用..... 37
使用可能な文字コード一覧..... 63
使用制約..... 105
初期調査資料..... 41
スーパーユーザー..... 15,109
正常稼働の通知メール..... 93
製品情報..... 30
接続先のサーバの情報..... 109
設定内容の確認..... 21
セットアップ..... 12
セットアップ中にトラブルが発生した場合の対処方法 114
セットアップの完了..... 22
セットアップの準備..... 12
セットアップ用PC..... 12

[た]

対処ウィンドウ..... 28
対処とリカバリー..... 31
端末の条件..... 60
調査資料の採取..... 41
デザインシート..... 112
電源状態の確認..... 96
電源制御..... 4,94
電源の投入..... 13,50,95
電源ボタン..... 14
電源ランプ..... 14
データベース以外の警告・エラー状態の通知メール..... 93
データベースインターフェース..... 21
データベースインターフェース設定..... 20
データベースインターフェースの確認..... 64
データベースインターフェースの初期化..... 65
データベースシステムの起動と停止..... 50
データベースの警告・エラー状態の通知メール..... 92
問合せ時に必要な情報..... 120
トラブルシューティング..... 114

[な]

内部ネットワーク..... 20
名前解決..... 24
ネットワークの変更..... 66

[は]

パスフレーズの初期値..... 82
バックアップ..... 35
バックアップジョブ..... 73
バックアップジョブの開始時刻..... 73
バックアップ製品..... 72
ハードウェア構成..... 1
ハードウェア部品交換..... 42
ファイアウォール..... 5
付属のDVD..... 2
保守..... 36
保守サービスについて..... 120
保守ランプについて..... 49
ホスト名の変更..... 80
[ホーム]画面..... 26

[ま]

マニュアル..... 30
メッセージ一覧..... 52
メッセージウィンドウ..... 28
メッセージの消去..... 70
メール通知..... 4,90
文字管理..... 4,93

[や]

容量増設オプション..... 9
容量追加..... 46

[ら]

リカバリー..... 31
リカバリー時間の算出で想定しているデータベース規模 34
リカバリー所要時間の目安..... 33
リカバリーボタン..... 28
リストアジョブ..... 77
ログアウト..... 29